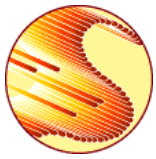


Sandstorm Enterprises

PhoneSweep® 4.4

User Manual

Sandstorm Enterprises, Inc.
PO Box 381548
Cambridge, MA 02238-1548
http://www.sandstorm.net
sales@sandstorm.net
support@sandstorm.net

Tel: 617-426-5056
Fax: 617-357-6042

July 18, 2002

[This Page Intentionally Blank]

Table Of Contents

Legal Notices **9**

End User License Agreement 9

1 Introduction **12**

1.1 Why Worry About Unsecured Modems? 12
1.2 PhoneSweep: A Better Telephone Line Scanner 12
1.3 New Features in PhoneSweep 4.4 13
1.4 Appropriate and Ethical Use of PhoneSweep 13

2 A Tour Of PhoneSweep **15**

2.1 The PhoneSweep Window 15
2.2 PhoneSweep Icon Quick Reference Chart 16
2.2.1 Top Horizontal Toolbar Icons 16
2.2.2 Vertical Toolbar Icons 17
2.2.3 Bottom Toolbar Icons 17
2.2.4 Results Tab Icons 18
2.2.5 Phone Numbers Tab Icons 19
2.3 PhoneSweep Configuration Options 19
2.3.1 Saving and undoing changes to configuration options 19
2.3.2 Popup Menus 19
2.4 Profiles 20
2.4.1 Number of Phone Numbers per profile Limits 20
2.4.2 MySQL 3.23.0 Limits on Profile Size, Number of Profiles 21
2.5 Dialing Rules 21
2.6 Levels of Effort 21
2.7 Brute Force Username/Password Guessing 22
2.7.1 Username/password recycling 23
2.8 Importing and Exporting PhoneSweep Data 23
2.9 Single Call Detect (SCD) 24
2.9.1 How SCD improves scan speed and accuracy 24
2.9.2 Many off-the-shelf modems support SCD 25
2.9.3 Modems that do not support SCD 25
2.10 Controlling when phone numbers are called 26
2.10.1 Time Periods 26
2.10.2 Using time periods to control the start of a scan 26
2.10.3 The Blackout period 27
2.10.4 Controlling Sweeps through the use of other Time Options 27
2.10.5 Schedule Sweep Start and Stop on the currently open profile 27
2.11 The phonesweep.ini File 27
2.12 Emergency Number Screening 27
2.13 Possible Testing Injuries 28

3 Installation and Setup **30**

3.1 System Requirements 30

3.1.1 Dialing Computer 30
3.1.2 Operating System 31
3.1.3 A cautionary note on laptop computers and Windows NT 31
3.1.4 Modem and multi-port serial I/O hardware recommendations 31
3.1.5 Modem Phone Line(s) 32
3.1.6 Security 32
3.2 TCP/IP 32
3.2.1 Issues with Windows 95A 32
3.2.2 Firewalls and TCP/IP 33
3.2.3 Software that can interfere with TCP/IP operation 33
3.3 Winsock 2 and HTML Help 33
3.4 Preparing to install and run PhoneSweep 34
3.5 Installing PhoneSweep 35
3.6 Hardware License Protection 35
3.6.1 Laptop models known to have problems with the dongle: 36
3.6.2 Software known to interfere with dongles on the parallel port 36
3.6.3 Instructions for installing the optional USB dongle 36
3.7 Selecting Modems for use with PhoneSweep 37
3.8 Recommended Modems 39
3.8.1 3.3v chipset Modems approved for PhoneSweep 3.01 and above 39
3.8.2 Other modems tested by Sandstorm 40
3.8.3 Modems Not Recommended 40
3.8.4 Modems recommended by customers in other countries 40
3.9 Recommended ISDN-capable modems 41
3.9.1 ISDN sweeps in foreign countries 41
3.10 Scanning in Multiple Countries 41
3.11 Testing COM ports, Modems using checkmodems.exe 42
3.12 Configuring your PC to support 4 or more Modems 43
3.12.1 IRQs and I/O addresses 43
3.13 Equipping a Desktop Computer with Multiple Modems 45
3.13.1 Installation advice for multi-port cards 45
3.14 Equipping a Desktop with multiple modems for PhoneSweep Plus 12 and 16 46
3.15 Equipping a Laptop with Multiple Modems 47
3.16 Uninstalling PhoneSweep 47
3.17 Reinstalling PhoneSweep 47

4 Setting Up a Sweep 48

4.1 Setting Up And Managing Calling Profiles 48
4.1.1 What information is contained in a profile? 49
4.1.2 Overview of profile management 50
4.2 Adding Phone Numbers to a Profile 50
4.2.1 What numbers can PhoneSweep call? 51
4.2.2 The Add Phone Numbers dialog box 52
4.2.3 Adding a single phone number or a range of phone numbers 53
4.2.4 Telling PhoneSweep when to call phone numbers (Time Periods) 54
4.2.5 Adding Notes for a single phone number or range of phone numbers 54
4.2.6 Editing and deleting phone numbers and associated time periods and notes 54

4.3 Setting Scheduled Start and Stop times 55
4.3.1 Schedule Sweep Start Time 55
4.3.2 Schedule Sweep Stop Time 55
4.3.3 Canceling Scheduled Starts and Stops 55
4.4 Setting Time Options 56
4.4.1 24-hour format 57
4.4.2 Redefining time periods 57
4.4.3 Redefining weekdays and weekends 57
4.4.4 Blackout periods 57
4.4.5 Setting time periods for imported phone numbers 58
4.4.6 Setting how long PhoneSweep will wait for a remote response 58
4.5 Setting up your Modems 59
4.5.1 Windows and your modem 60
4.5.2 Configuring the Modems sub-tab 60
4.6 Setting Level of Effort 62
4.6.1 What does PhoneSweep do at each level of effort? 63
4.6.2 Username/password recycling 64
4.6.3 Using multiple profiles to optimize large scans 64
4.6.4 Find Modems First 65
4.6.5 Limiting numbers of calls and brute-force attempts 65
4.6.6 The *bruteforce.txt* file 65
4.6.7 Using *brutecreate.exe* to customize *bruteforce.txt* 67
4.7 Setting Dialing Options 69
4.7.1 Setting dialing prefix and suffix 70
4.7.2 Sequential scanning 70
4.7.3 Setting PPP mode 70
4.7.4 Emergency Number (911) screening 71
4.7.5 Redialing busy numbers 71
4.7.6 Setting modem baud rate 71
4.7.7 Setting Single Call Detect (SCD) mode 71
4.7.8 Setting single call voice timeout 72

5 Sweeping 73

5.1 Setting Up A Test Sweep 73
5.2 Before You Start Your Sweep 73
5.3 Starting Your Sweep 74
5.4 Starting and Ending a Sweep Automatically 74
5.5 Sweeping for ISDN devices 75
5.6 Monitoring Your Sweep in Real Time 75
5.6.1 Estimated Progress 76
5.6.2 Actual Progress 77
5.6.3 Modem Status 77
5.6.4 Why might a modem become “disabled”? 77
5.7 Monitoring Recent Events: The History Tab 77
5.8 Viewing Your Results 79
5.8.1 Timestamps 79
5.8.2 Categories of results 80

5.8.3 Identification of remote systems 81
5.9 Rescanning a Profile 81

6 Importing and Exporting Data 82

6.1 Importing Phone Number Lists 82
6.1.1 Formatting imported phone numbers 82
6.1.2 Importing Phone Numbers with associated Notes 83
6.1.3 Time Period codes 83
6.1.4 Default Import Time Period 84
6.2 Importing Brute Force Information 84
6.2.1 Formatting imported Username/Password pairs 85
6.3 Exporting Data 86
6.3.1 Exporting Call History 86

7 Generating PhoneSweep Reports 89

7.1 Selecting Standard Report Sections 89
7.1.1 Anomaly Detection 90
7.1.2 Penetrated Modem Responses 90
7.1.3 Appendix A: All Responses From Target Modems 90
7.1.4 Appendix B: Phone Number Taxonomy 90
7.1.5 Appendix C: List of All Calls and Their Results 91
7.1.6 Binary bytes and replacing unprintable characters 91
7.2 Customizing Your Report Template 91
7.2.1 Report Sections 91
7.2.2 Report variables in ReportTemplate.RTF 92

8 Differential Reporting 94

8.1 What information is in a differential report? 94
8.1.1 Heading 95
8.1.2 Engineering Summary 95
8.1.3 Full Call History Change Report 95

9 Graphing Call History Results 96

10 Evaluating the Results of Your Scan 97

10.1 Expected Sweep Result Charts 97
10.1.1 Voice Line Sweep Results 98
10.1.2 Fax Line Sweep Results 98
10.1.3 Modem Line Sweep Results 98
10.1.4 Fax/Modem Line Sweep Results 99
10.1.5 Second Dial-tone Sweep Results 99
10.2 Characteristics of telephone systems that can affect the results of a scan 99
10.3 Threats posed by various devices and situations 100
10.3.1 Data-only modems 100
10.3.2 Fax/modems 100
10.3.3 Fax machines 100
10.3.4 Combination answering machine/fax 101

10.3.5 Numbers that report "VOICE" 101
10.3.6 Fax machine issues 101
10.3.7 Incorrectly configured software 101
10.3.8 Numbers that consistently time out 101
10.3.9 Default passwords 102
10.3.10 Second dial tones 102
10.3.11 Numbers that are always busy 102
10.4 Mis-identifications 102
10.4.1 Fax machines known to generate mis-identifications 102
10.4.2 Situations that may generate false Penetration results 103
10.4.3 Other situations that generate mis-Identifications 103

11 Customizing PS Defaults Using the PhoneSweep.INI file 104

Appendix A: Glossary 107

Appendix B: PhoneSweep FAQ 113

Single Call Detect (SCD) 113
Using PhoneSweep 113
Improving PhoneSweep's Performance 116
Fax machines and Fax/Modems 117
Finding All the Modems 117
Evaluating Security Risks 118
The PhoneSweep Report 119
Ethical Considerations 119
Miscellaneous Questions 119

Appendix C: PhoneSweep Troubleshooting Guide 121

Information To Collect Before Troubleshooting 121
Things To Check If You're Having Trouble 122
Common Problems and Possible Solutions 123
PhoneSweep Error Messages 128
Error messages on install 128
Error messages on program startup 129
Error messages regarding the dongle 130
Error messages when starting a sweep 130
Error messages on the Status tab 130
Error messages on the History tab 131
User interface error messages 131
The debug.bat File and Advanced Debugging 131
I've Tried Everything and PhoneSweep Still Doesn't Work! 132

Appendix D: Contacting Sandstorm 133

About Technical Support for PhoneSweep 133
Submitting Bug Reports 133
Before You Contact Sandstorm Technical Support 133
Contacting Sandstorm Technical Support 134

Contacting Sandstorm Sales 134

Appendix E: Architecture and the Command Line 135

Running PhoneSweep from MS-DOS 135
PhoneSweep Command Line Arguments 135
Environment Variables 136

Appendix F. Sample *brutecreate.exe* Output File. 137

Appendix G: A Sample Standard PhoneSweep Report 139

Appendix H: A Sample Differential PhoneSweep Report 145

Appendix I: Miscellaneous 147

Password Security 147
List of Identified Systems 148
Important Web sites and Phone Numbers 153

Legal Notices

Danger Warning: This program, PhoneSweep, is designed to test computer system security on telephone networks. It may be used by authorized personnel only, and only when requested by the computer system owners. Any other use may be illegal, or cause injury or financial loss.

PhoneSweep may only be used by authorized licensees, who agreed upon installation to all of the terms and conditions of the end user license below:

End User License Agreement

Sandstorm Enterprises Inc. ("Sandstorm") and/or its suppliers own these programs and their documentation, which are protected under applicable copyright laws. Your right to use the programs and the documentation is limited to the terms and conditions described below.

1. License: YOU MAY: (a) use the enclosed programs on a single computer; (b) physically transfer the programs from one computer to another provided that the programs are used on only one computer at a time, and that you remove any copies of the programs from the computer from which the programs are being transferred; (c) make a copy of the programs solely for purposes of backup. The copyright notice must be reproduced and included on a label on any backup copy.

Sandstorm reserves all other rights, including, but not limited to, the following:

YOU MAY NOT: (a) distribute copies of these programs or their documentation to others; (b) rent, lease or grant your rights to others; (c) alter the programs or their documentation without the prior written consent of Sandstorm; (d) disassemble or reverse-engineer the programs; or (e) ship or transmit (directly or indirectly) any copies of the programs or its media, or any direct product thereof, to any country or destination prohibited by the United States Government.

2. Term: Your License remains effective until terminated. You may terminate it at any time by destroying the distribution media together with all copies of the programs in any form, and returning the hardware license management device (“dongle”) to Sandstorm or destroying it if returning it is not possible. Your License will also automatically terminate without notice if you fail to comply with any term or condition of this Agreement. Upon termination you must destroy all copies of the programs in any form.

3. Limited Warranty, Disclaimer and Limitation of Liability: Sandstorm and Vendor warrant the media on which the Licensed Programs are provided to be free from defects in materials and workmanship for 90 days after delivery. Defective media may be returned for replacement without charge during the 90-day warranty period unless the media has been damaged by accident or misuse. Due to the complex nature of computer software, Sandstorm does not warrant that the Licensed Programs are completely error-free, will operate without interruption, or are compatible with all equipment and software configurations. DO NOT USE THE LICENSED PROGRAMS IN ANY CASE WHERE SIGNIFICANT DAMAGE OR INJURY TO PERSON, PROPERTY OR BUSINESS MAY HAPPEN IF ANY ERROR OCCURS. YOU EXPRESSLY ASSUME ALL RISK FOR SUCH USE, AND FOR ANY VIOLATION OF STATE OR FEDERAL LAW THAT MAY RESULT.

Repair, replacement or refund (at the option of Sandstorm) is the exclusive remedy if there is a defect. SANDSTORM MAKES NO WARRANTIES, EXPRESSED OR IMPLIED, WITH RESPECT TO THE LICENSED PROGRAMS, THEIR MERCHANTABILITY, OR THEIR FITNESS FOR ANY PARTICULAR PURPOSE. IN NO EVENT WILL SANDSTORM BE LIABLE FOR INDIRECT OR CONSEQUENTIAL DAMAGES, INCLUDING, WITHOUT LIMITATIONS, LOSS OF INCOME, USE OR INFORMATION, NOR SHALL THE LIABILITY OF SANDSTORM EXCEED THE AMOUNT

PAID FOR THE LICENSED PROGRAMS. THE LICENSED PROGRAMS ARE NOT INTENDED FOR PERSONAL, FAMILY OR HOUSEHOLD USE.

Any suit or other legal action relating in any way to this Agreement or to the Licensed Programs must be officially filed or officially commenced no later than one (1) year after it accrues. This warranty gives the customer specific legal rights, and you may also have other rights, which vary from state to state.

4. General terms: The License shall not be assigned or transferred without the written consent of Sandstorm. The validity, construction and performance of this Agreement are governed by the laws of the Commonwealth of Massachusetts, without regard to Massachusetts's choice-of-law rules. Suit or arbitration relating to this Agreement may be brought only in Massachusetts.

5. HIGH RISK ACTIVITIES. YOU ACKNOWLEDGE THAT YOU MAY USE THE LICENSED PROGRAMS TO PERFORM INHERENTLY DANGEROUS ACTIONS, WITH A SIGNIFICANT RISK OF: (a) SUBSTANTIAL INJURY OR LOSSES TO YOUR COMPUTER SYSTEMS, BUSINESS OPERATIONS, AND OTHER PROPERTY, OR TO THE INTERESTS, RIGHTS, PROPERTY OR WELL-BEING OF THIRD PARTIES, INCLUDING BUT NOT LIMITED TO YOU OR PEOPLE OR BUSINESSES ASSOCIATED WITH YOU, OR (b) VIOLATING THE LAW (ALL SUCH INJURY, LOSSES AND VIOLATION ARE REFERRED TO AS "TESTING INJURIES"). YOU HEREBY ASSUME ALL RISK OF TESTING INJURIES, WITHOUT REGARD TO WHETHER SANDSTORM KNEW OF OR COULD HAVE PREVENTED SUCH INJURIES.

YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS. YOU FURTHER AGREE THAT IT IS THE COMPLETE AND EXCLUSIVE STATEMENT OF THE AGREEMENT BETWEEN YOU AND SANDSTORM, AND SUPERSEDES ANY EARLIER PROPOSAL OR PRIOR ARRANGEMENT, WHETHER ORAL OR WRITTEN, AND ANY OTHER COMMUNICATIONS BETWEEN YOU AND SANDSTORM RELATING TO THE SUBJECT OF THIS AGREEMENT.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). Those routines are copyright 1995-1997 Eric Young. The following is included in Mr. Young's copyright notice:

Copyright (C) 1995-1997 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)."

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

Our Thanks to Eric Knight who gave us permission to use his publicly available Default System Passwords as part of our suite of bruteforce password source files. The original URL for Eric Knight's password list can be found at: http://www.securityparadigm.com.

1 Introduction

Welcome to PhoneSweep!

PhoneSweep® is a telephone system security audit tool that searches for modems, fax machines, and other devices within a set of phone numbers. PhoneSweep can identify security risks such as unsecured modems and potential vulnerability to toll fraud.

1.1 Why Worry About Unsecured Modems?

The presence of unsecured or misconfigured modems attached to computers on your network can undermine a well thought-out security plan. Persons unaware of the risks may set up modems on their computers that can be accessed with either no password or an easily guessed password. These modems are then vulnerable to computer criminals who "war dial," or call numbers systematically until they find a phone number that connects to an unsecured dialup.

If a computer with an unsecured modem is connected to your organization's network, anyone with a little computer skill and malicious intent can use that unsecured modem as a "back door" into your network. Firewalls don't protect a network against this type of attack because the intruder comes in over phone lines, rather than over the Internet, bypassing firewalls.

Obviously, it is in your and your organization's best interest to use PhoneSweep to find rogue modems and shut them down before an attacker finds them.

1.2 PhoneSweep: A Better Telephone Line Scanner

Before the introduction of PhoneSweep, there were no reliable tools for conducting security audits of telephone systems. Security professionals who wanted to find unsecured modems had to resort to using "war dialers," publicly available programs written by amateur programmers and designed to commit illegal acts. These tools are generally unsupported, difficult to use, and have limited reporting capabilities. Many, such as ToneLoc, work only under DOS. Furthermore, freeware dialers may contain undocumented "features" such as viruses or "back doors." Do you really want to trust your network security to the product of an anonymous amateur programmer whose intent was toll fraud?

PhoneSweep was designed and written specifically as a security audit tool by an experienced team of engineers and security professionals. PhoneSweep is designed to be easy to use, flexible, and powerful.

PhoneSweep:

- Runs on industry-standard Windows 95, 98, NT, 2000 and XP platforms.
- Has an intuitive, easy-to-use graphical user interface.
- Is capable of brute-force user name/password guessing (penetration testing) against many of the systems it encounters, including PPP systems.
- Produces detailed, customizable reports.
- Comes in versions that can dial with one, four or eight modems.
- Allows you to Stop and Restart scans on each profile without losing data.

1.3 New Features in PhoneSweep 4.4

The significant new features of PhoneSweep 4.4 are:

- Supports newer version of Conexant chipset.
- The bruteforce username/password list can now be viewed and edited from the **Effort** tab.
- New option to run a report after a sweep is complete.
- New option on license screen to start with a new or different profile.
- New right-click popup menu on **Modems** and **Status** tabs allows reset of modems, and setting of options for all modems (on **Modems** tab).
- Right-click popup menu on the **Phone Numbers** tab now includes an option to open all phone numbers' call results.
- The *debug.bat* utility includes an option to run *dbfix.exe* (fixes a corrupted database).
- User is warned if running on a battery only.
- Better handling of power management events. PhoneSweep will attempt to stop a running sweep if machine goes into standby mode. (This may not be supported on all hardware.)
- Charts now work under Office XP.
- More improvements in profile loading time.
- More system identifications.

1.4 Appropriate and Ethical Use of PhoneSweep

With PhoneSweep, organizations can easily and legally audit their own phone systems. However, PhoneSweep is a powerful tool, and any powerful tool can potentially be misused. Be sure that you have read and fully understand the PhoneSweep End User License Agreement, and be certain that you have clear permission to scan any phone numbers before you scan them. **Scanning phone numbers that you are not authorized to scan may be illegal in your area of operation.**

Sandstorm Enterprises prohibits any use of PhoneSweep that is expressly forbidden or forbidden by implication in the End User License Agreement. **PhoneSweep requires that you agree to the End User License Agreement every time you run the program.** Sandstorm Enterprises expressly disclaims any responsibility for any event resulting from the use or misuse of PhoneSweep.

You may hear PhoneSweep referred to as a "war dialer." This term entered popular culture after the 1983 film *War Games*, and describes a type of computer program that automatically dials phone numbers to search for unsecured modems. During the 1980's, many simple war dialers were written by so-called "phone phreaks" looking for vulnerable systems to attack or 800 number extenders that could be used to commit toll fraud.

Sandstorm Enterprises refers to PhoneSweep as a "Telephone Line Scanner" to distinguish it from programs designed to commit illegal acts. It is legal, ethical and wise to use PhoneSweep to test your own phone systems for insecure modems. ***It is possibly illegal, and definitely not ethical, to use PhoneSweep to look for vulnerabilities in phone systems that you are not authorized to scan.***

Sandstorm Enterprises realizes that it is important that PhoneSweep not be usable by unauthorized persons. For this reason, PhoneSweep is supplied with a hardware license management device known as a "dongle" that attaches to a computer's parallel or USB port. **PhoneSweep will not make calls unless the**

dongle is attached. This helps protect PhoneSweep from unauthorized use within your organization, or theft or piracy by people outside your organization.

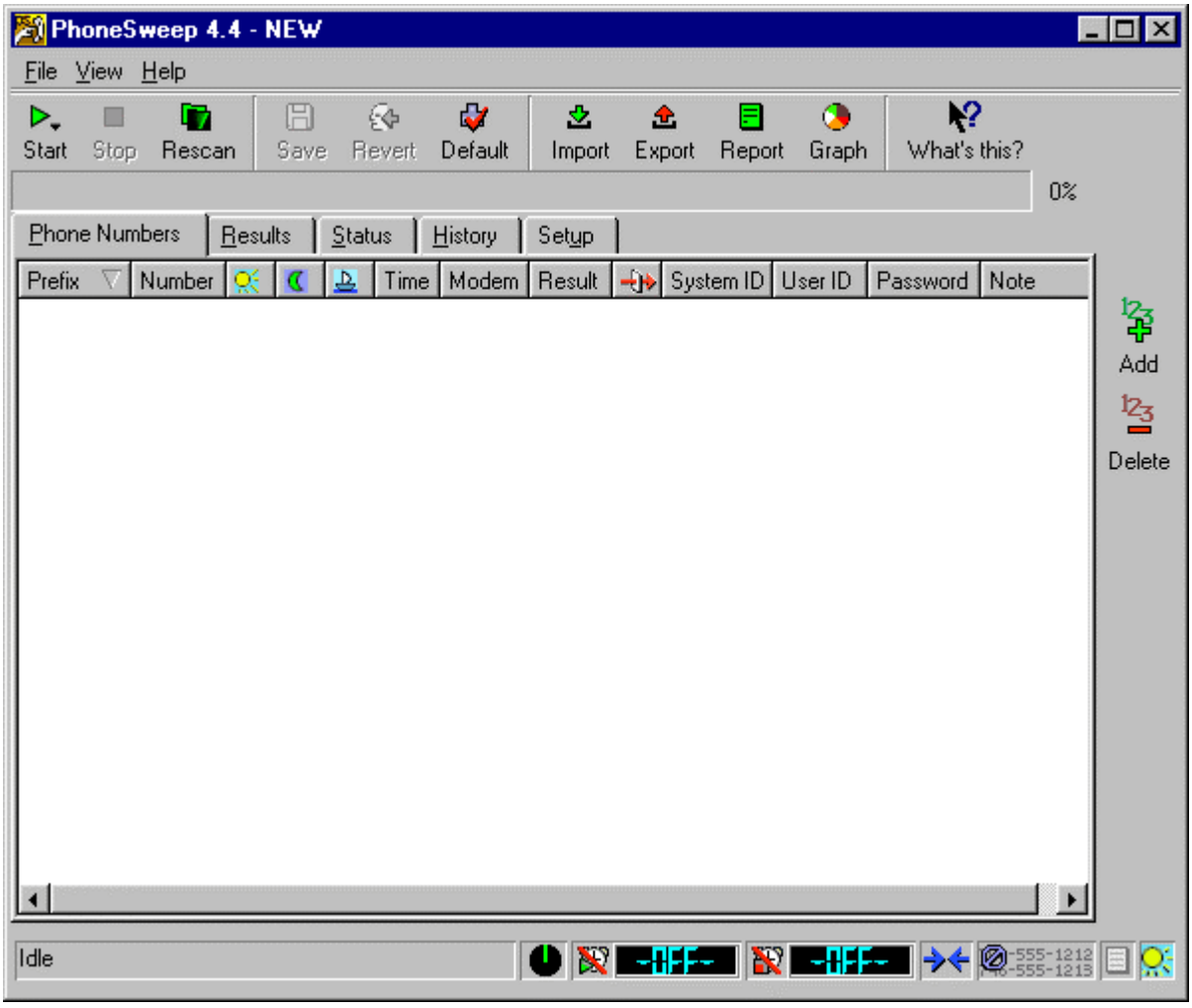
2 A Tour Of PhoneSweep

The concept behind PhoneSweep is simple. PhoneSweep uses one or more modems to place calls to a specified list of phone numbers. If a call to a remote phone number is answered, PhoneSweep collects and records information about the answering device.

PhoneSweep is highly configurable and offers advanced features such as system identification, brute force username/password guessing, and customizable reporting.

2.1 The PhoneSweep Window

The PhoneSweep user interface is designed so that finding what you want is like looking through a card file.



Take a moment to familiarize yourself with features of the PhoneSweep window:

- **Pull-down menus**: the File, View and Help menus.
- **Horizontal toolbar**: this button bar allows you to easily control your scan and to save or discard customizations.
- **Percent Done bar**: this thick dotted blue line indicates how far your current scan has progressed. On the right hand side, Phone Sweep provides the percentage of the scan that has been completed - in this case 0%.
- **Tabs and Sub-tabs**: The **Phone Numbers**, **Results**, **Status**, **History**, and **Setup** tabs can be clicked on to allow you to view and modify information associated with your scan. If you click on the **Setup** tab, a second row of tabs, called *sub-tabs*, will appear will appear just below the primary row of tabs.
- **Vertical toolbar**: these buttons on the right of the PhoneSweep window change with the particular tab or sub-tab selected, and allows you to control functions of the selected tab or sub-tab only.
- **Action dialog**: the small window at the bottom left of the PhoneSweep displays functional messages showing PhoneSweep's current operations.
- **Status icons**: the small icons at the bottom right of the PhoneSweep window show whether PhoneSweep is scanning, whether or not the current open profile has a scheduled sweep start and/or stop time, whether numbers are available to dial, the level of effort, report generation status, and the current time period.

2.2 PhoneSweep Icon Quick Reference Chart

These icons appear in the PhoneSweep window to show status or indicate which operations you can perform. More detailed explanations can be found in the appropriate sections of the manual.

2.2.1 Top Horizontal Toolbar Icons

Icons on the top horizontal toolbar control major functions.

	Start	Click on this button to begin a sweep. Press and hold down this button to schedule Start and Stop times for a sweep on current open profile.
	Stop	Click on this button to stop a sweep. Press and hold down this button to schedule Start and Stop times for sweep on current open profile.
	Rescan	Click on this button to create and name a clone of the current profile (minus the Call History), and open it as the current profile ready to dial the numbers anew.
	Save	Save changes to the current profile, including the new settings.
	Revert	Revert to last saved settings for all variables in all sub-tabs
	Default	Resets all variables on all sub-tabs to their default settings.
	Import	Import phone numbers into current open profile or username/password list into *bruteforce.txt*.
	Export	Export call results (all or by result), phone numbers, or Usernames/Password lists.

	Report	Generate a standard report based on the information in the current profile, or a differential report based on the results of two separate profile sweeps.
	Graph	Generate a pie graph based on the information in the current profile (requires Excel 2000).
	What's This?	Click on this icon; then point at a feature on the PhoneSweep User Interface to identify that item.

2.2.2 Vertical Toolbar Icons

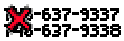
Icons on the vertical toolbar on the right side of the PhoneSweep windows show options related to each tab. The contents of the vertical toolbar vary with the particular tab or sub-tab that is selected, and on some tabs the vertical toolbar does not appear at all.

	Open profile	Open a pre-existing profile (**Profile** sub-tab).
	New profile	Create a new profile (**Profile** sub-tab).
	Copy profile	Prompt the user for a name for the new profile and copy the contents (minus Call History and with all settings at default values} of the current profile into it (**Profile** sub-tab).
	Delete profile	Delete a profile and all its associated information (**Profile** sub-tab).
	Save Profile Note	Save changes made to note associated with the highlighted profile name (**Profile** sub-tab).
	Undo Note changes	Undo UNSAVED changes to Profile Note (**Profile** sub-tab).
	Freeze	Stop the real-time display on the **History** tab without stopping the current scan.
	Thaw	Restart the real-time display on the **History** tab.
	Clear	Clear the screen display of its current contents (**Add Phone Numbers** dialog box and **History** tab).
	Add	Add a phone number or range of numbers to the current profile (**Phone Numbers** tab – Calls **Add Phone Numbers** dialog box).
	Delete	Delete a phone number or range from the current profile (**Phone Numbers** tab).
	Add/Save	Add/Save phone number or range of phone numbers (**Add Phone Numbers** dialog box).

2.2.3 Bottom Toolbar Icons

Icons at the bottom of the PhoneSweep window show status.

	Initializing	PhoneSweep is preparing to accept user input.
	Idle	PhoneSweep is not dialing and is ready to accept user input.
	Sweeping	PhoneSweep is in the process of performing a sweep.
	Connect	At this Level of Effort, PhoneSweep will connect to and immediately disconnect from any device found while sweeping (also on **Effort** sub-tab).
	Identify	At this Level of Effort, PhoneSweep will attempt to determine the type of

		operating system running on devices it has connected to (also on **Effort** sub-tab).
	Penetrate	At this Level of Effort, PhoneSweep attempts to identify remote systems and then executes a brute-force attempt to log on to systems it has identified (also on **Effort** sub-tab).
	Ready to dial	There are numbers in the active profile that can be dialed during the current time period and have not yet been dialed.
	No numbers to dial	PhoneSweep cannot place any more calls in the present time period. Either no phone numbers have been set to be called at the present time, or all numbers that are callable in this time period have been dialed.
	No numbers in profile	There are no telephone numbers in the current calling profile.
	Report idle	PhoneSweep is not in the process of generating a report.
	Generating report	PhoneSweep is in the process of making a report on the results of a sweep.
	Business hours	A customizable time period defaulting to 9 AM to 5 PM on weekdays. Only phone numbers marked as callable during Business hours will be called while this icon is displayed (also on **Phone Numbers** tab).
	Outside hours	A time period made up of the parts of a weekday that are not Business Hours (default is midnight to 8:59AM, and 5:01PM to midnight. Only phone numbers callable during Outside Hours will be called while this icon is displayed (also on **Phone Numbers** tab).
	Weekend	A customizable time period defaulting to all day Saturday and Sunday. Only phone numbers that are callable during Weekend hours will be called while this icon is displayed (also on **Phone Numbers** tab).
	Start Time Scheduled	Start time has been scheduled for the current profile.
	Stop Time Scheduled	Stop time has been scheduled for the current profile.
	No Scheduled Start Time	No start time scheduled for current profile.
	No Scheduled Stop time	No stop time scheduled for current profile
	Scheduled Sweep Start (Off)	(Icon on the left) No Scheduled Sweep Start time for current profile
	Scheduled Sweep Stop (off)	(Icon on the right) No Scheduled Sweep Start time for current profile

2.2.4 Results Tab Icons

Icons on the Results tab classify call results.

	There aren't any numbers that fall into this particular category.
	One or more numbers fall into this category. Click the icon to see a full listing.

2.2.5 Phone Numbers Tab Icons

Icons on the Phone Numbers tab show status by phone number.

	There have not been any calls to this phone number.
	For a prefix, indicates that there are individual phone numbers grouped within this prefix. Click on the icon to list the phone numbers using the prefix. For a phone number, there have been calls to this number. Click on the icon to see a record of all calls.

2.3 PhoneSweep Configuration Options

PhoneSweep's primary control features can be reached either through pull down menus, buttons and Pop-up Menus (Sweep **Stop**, **Start**, Generate **Chart** or **Report**, etc). Settings affecting the make up of individual profiles (Profile Contents, Call Parameters, Call Progress, Profile Management, etc.) are accessed through tab and sub-tab windows, as well as pop-up menus.

2.3.1 Saving and undoing changes to configuration options

You must use the **Save** button on the horizontal button bar to save any changes you have made to items on a tab or sub-tab. **Changes will not take effect until they have been saved!** PhoneSweep will warn you if you start a sweep with unsaved changes, but it will not issue warnings if you change settings after starting a sweep.

Note that you can also save changes using the **Save** option under the **File** menu.

The **Revert** button will return all sub-tabs to the last saved settings. The **Default** button will change settings on all tabs and sub-tabs to their original (default) settings. Use the **Default** button with caution! When it is used, any changes you have made are immediately lost, without use of the **Save** button. You cannot use the **Revert** button to undo changes made with the **Default** button. The **Default** settings can be changed by editing the *PhoneSweep.ini* file; see Section 11, **Customizing PS Defaults Using the PhoneSweep.INI file**.

2.3.2 Popup Menus

Some additional view or configuration control options are only accessible through pop-up menus by right-clicking over the main viewing area on most tabs and sub-tabs.

- **Phone Numbers tab: Alter** (time periods and/or notes) for highlighted phone numbers or prefixes, or all phone numbers; **Show Call Detail** on individual call result, **Expand** or **Collapse** all or just highlighted prefixes or phone numbers, and **Find** a given number or call result, or any number or result matching a subset (phone numbers and call results must be loaded on the **Phone Numbers** tab by expanding the tree, in order to search for them).
- **Results tab: Show Call Detail** on individual call result, **Expand** or **Collapse** all or just highlighted call result folders, and **Find** a given number, or any number matching a subset, and **Find** a given number or call result, or any number or result matching a subset.
- **Status tab: Reset** one or all modems.
- **History tab: Show Call Detail** on individual call result, and **Find** a given number or call result, or any number or result matching a subset.
- **Setup->Profiles sub-tab Profile Notes area: Text Editing options** for profile notes section.

- **Setup->Modems tab: Use a setting** for all modems**, Renumber COM ports, Reset** one or all modems.

You can also access additional scheduling features by selecting and holding either the **Stop** or **Start** button (whichever button is not grayed out at the time) until a pop-up window appears. Scheduling is also available from the **File** menu.

2.4 Profiles

"Profiles" are PhoneSweep's basic unit of information storage. Each profile is a database containing a set of phone numbers to scan, as well as the time periods during which to scan them and associated notes and associated scan configuration options. Every profile also saves the scan results for each phone number as they are scanned. This means **you can stop and restart scans without losing data.** You can even stop scanning one profile, switch to another profile to scan, then later stop and switch back to the first profile so you can resume scanning that one.

You can have as many profiles as you have memory to hold them. (MySQL can handle up to 5,000,000 (5 million) records).

Each profile you create includes:

- A **list of telephone numbers, with associated time period and notes**. You can have either a range of phone numbers or several individual, non-consecutive phone numbers. **Note:** Time periods and notes are configurable on the **Phone Numbers** tab. You can either add or import telephone numbers and scan parameters from pre-made files or from other applications.
- A **list of username/password pairs to use in brute-force password guessing attempts.** These are configurable in the *bruteforce.txt* file or by using brutecreate.exe; or you can import a new .txt file. As of PhoneSweep 4.4 you can also view and edit them via the Effort tab.
- The **results of each telephone call.** These are viewable on either the **Results** tab by *Call Result type*, or on the **Phone Numbers** tab by expanding each phone number.
- **Configuration information** associated with that profile.

2.4.1 Number of Phone Numbers per profile Limits

You can have as many profiles as you want in your PhoneSweep database; however, there are limits on how many numbers you can have in each profile, and what Sandstorm will support:

- PhoneSweep Basic has a hard limit of 800 phone numbers allowed per profile.
- PhoneSweep Plus and Plus 8 each have a soft limit of 10,000 phone numbers per profile.
- PhoneSweep Plus 12 and Plus 16 each have a soft limit of 20,000 phone numbers per profile.

The hard limit for PhoneSweep Basic profiles means PhoneSweep will not allow you to have more than 800 numbers in any profile. The soft limit on other versions of PhoneSweep means that users can add up to 10,000 or 20,000 numbers at a time; however, you can have more than 10,000 or 20,000 in each profile.

Please remember that if you have more than the supported phone number of phone numbers in your profiles that Sandstorm does not guarantee satisfactory results. At the very least, you will need to increase both your CPU and RAM capacities.

2.4.2 MySQL 3.23.0 Limits on Profile Size, Number of Profiles

The MySQL database that PhoneSweep uses allows you to have a large number of profiles of varying size (up to 50,000,000 records for MySQL version 3.23.0). **Please Note:** Sandstorm does not guarantee satisfactory results with large numbers of profiles or profiles over 10,000 numbers for PhoneSweep Plus and Plus 8 and 20,000 numbers for Plus 12 and 16.

Scans on profiles that contain more than the recommended number of phone numbers may suffer from performance problems, particularly on slower PCs. Large profiles are also harder to recreate should they become damaged during a system crash or power outage. We recommend that you always save copies of your Profiles (Profile folders located in the folder named "Profiles" in the PhoneSweep directory) in a separate location and use the best processing power available.

For more information about configuring and managing profiles, please see **Setting Up And Managing Calling Profiles** in section 4.1.

2.5 Dialing Rules

Persons conducting telephone system security audits for an organization have a responsibility to minimize any inconvenience to members of the organization. To this end, PhoneSweep implements *dialing rules* that specify PhoneSweep's calling behavior such that the scan will have minimal impact on your organization's operations. Dialing rules control the order, time, and frequency of calls.

PhoneSweep can be instructed to:

- **Not make any calls during a specified interval**. For example, in some organizations, calls placed after hours to any number in the organization may be routed to a single point, such as a security desk. Obviously, it is both uninformative and damaging to make calls during such an interval.
- **Call a specified number or group of numbers only during certain intervals.** Telephone security auditors will want to schedule sweeps for times when they will be minimally disruptive. For example, someone conducting a sweep of university phone numbers may want to dial numbers that reach student dorms during the day and numbers that reach labs and offices during the evening.
- **Only call a given number a limited number of times per day.** This can be used to minimize disruption, and is especially important when running PhoneSweep at the Penetrate level of effort.
- **Stop retrying busy numbers after a specified number of calls.**
- **Call numbers either in sequence or randomly.**
- **Wait a specified amount of time between calls.** (**Note:** Never go below 5 seconds between calls, as it does not allow modems enough time to reset to make the next call).
- **Stop brute-force username/password guessing attempts after a specified number of tries**. Some computer systems will lock a user out of his or her account if too many unsuccessful login attempts are recorded.

More detailed information on how to take advantage of PhoneSweep's implementation of dialing rules appears in the appropriate sections of this manual.

2.6 Levels of Effort

You can specify the amount of information that PhoneSweep collects about the devices it encounters during a sweep by setting PhoneSweep to sweep at one of three **Levels of Effort** on the options **Setup-**

>Effort sub-tab. Once set, PhoneSweep's current level of effort is indicated by an icon at the bottom of the PhoneSweep window, as well as displayed on the **Setup->Effort** sub-tab. The three levels of effort available are:

- **Connect**. When this level of effort is specified, PhoneSweep will call each telephone number, classify the answer (if any) as Voice, Modem, Fax, etc. and then hang up. At Connect level of effort, *PhoneSweep listens only; no information is exchanged*.
- **Identify**. When this level of effort is specified, PhoneSweep will attempt to determine the specific type of device or operating system that has answered the call. *This may involve sending data (usually carriage returns) to the remote device to elicit a response*.
- **Penetrate**. When this level of effort is specified, PhoneSweep will call each modem that is at least partially identified and execute a brute force username/ password guessing attempt. Note that the Penetrate level of effort can be dangerous due to its intensive attempts to break into systems. Make sure you have clear authorization to be this intrusive before using PhoneSweep to scan a set of phone numbers in Penetrate mode, and that all calls are set up for the correct time period.

Levels of effort are cumulative. At a given level of effort, PhoneSweep will take the actions specified by that level of effort, as well as those specified by all less invasive levels of effort. For example, you must connect to a device before you can attempt to identify it. Likewise, if PhoneSweep is set to attempt to log in to a remote system, it will also attempt to identify the system. **Note** that PhoneSweep can only brute-force a system for which it has made at least a partial identification.

The level of effort you specify determines the number of phone calls PhoneSweep will make in order to complete the scan and, therefore, the time required by the scan. PhoneSweep running in Penetrate mode will make more calls than PhoneSweep running in Connect or Identify mode, since PhoneSweep will need to call back the modems it has identified in order to try the username/password combinations. You can use levels of effort to decrease the amount of time necessary to complete an audit by first sweeping a profile at the Connect level of effort, and then calling back numbers with suspicious responses at a higher level of effort.

For more information on setting the level of effort for a PhoneSweep scan, see Section 4.6, **Setting Level of Effort.**

2.7 Brute Force Username/Password Guessing

If the level of effort is set to Penetrate, PhoneSweep will attempt a username/password guessing attack on each modem it discovers. These username/password combinations are usually simple, and therefore easily guessed, such as:

"root"	"toor"
"system"	"manager"
"guest"	"guest"

The username/password list can be modified directly via the Effort tab (See Section 4.6.6, **The bruteforce.txt file** for more information). PhoneSweep comes with the following files and utilities for brute force username/ password guessing:

- ***bruteforce.txt:*** This is the file PhoneSweep uses to make username/password guesses. You will likely need to modify this file for your particular needs, which can be done using the *brutecreate.exe* utility or by directly editing the file. You can also import other

username/password files for PhoneSweep to use (please see Section 6.2, **Importing Brute Force Information**.)

- ***systemdefault.txt:*** This file contains a master list of default user name/passwords used by many common operating systems, that you can use as a resource to verify that the default user name/password setting on the systems in your workplace have been changed.. To use this file, you search it for the lines containing information on systems found on your network, then copy and paste the relevant lines into the bruteforce.txt or a new document that you can import as a user name/password source.
- ***brutecreate.exe:*** This MS-DOS command line utility combines usernames and passwords from separate files to add or replace the contents of the *bruteforce.txt* file. You can use the following password source files in combination with your own USERID sources files to customize *bruteforce.txt* with brutecreate.exe:
    - ***largebrute.txt*:** This file contains a dictionary of passwords that hackers commonly use.
    - ***largebruteback.txt:*** This file contains the same dictionary words as *largebrute.txt*, but each of them is backwards.

2.7.1 Username/password recycling

During Penetrate-level ( ) sweeps, username/password combinations can be *recycled* (used once against every modem PhoneSweep encounters), or *not recycled* (used only once during a scan, on the assumption that all modems share the same username/password database).

Not recycling usernames/passwords reduces the total number of calls that need to be made, and is recommended when all phone numbers being swept are connected to the same system. On the other hand, specifying that PhoneSweep should recycle username/password combinations will cause the scan to take longer, but make the scan more complete

For more information on when username/password recycling is useful and appropriate, see Section 4.6.2, **Username/password recycling**.

2.8 Importing and Exporting PhoneSweep Data

PhoneSweep is capable of importing and exporting several types of data.

You can enter phone numbers in a different program and have PhoneSweep import them. Imported phone numbers must be in text files and in one of the following formats.

- <phone number> <*Tab*> <time period code> <*CRLF*>
- <phone number> <*Comma Space*> <time period code> <*CRLF*>
- <phone number> <*Space Space*> <time period code> <*CRLF*>
- “<phone number”> <comma>”<time period code>”<CLRF>

To import a file containing a list of phone numbers, click on the **Import** button. When the **Import Dialog** box appears, enter the name of the file containing the list of phone numbers, select the **Phone numbers** Import Option, and then click OK. See Section 6.1, **Importing Phone Number Lists,** for more information.

You can also import Username/password combinations for use in the *Penetrate* level of effort using the **Import** button. For more information, see Section 6.2.

Finally, you can also export PhoneSweep-generated data such as phone numbers and call results using the **Export** button. See Section 6.3, **Exporting Data**, for more information.

2.9 Single Call Detect (SCD)

Single Call Detect (SCD) is a unique PhoneSweep feature that speeds telephone scanning and improves the accuracy and detail of information collected in the scan. In SCD mode, PhoneSweep listens to and evaluates each telephone call as it is made, and modifies its calling behavior accordingly.

Single Call Detect:

- Reduces the total number of calls that are needed to complete a scan
- Allows faster voice recognition (Voice lines are called just once).
- Decreases the probability of some testing injuries
- Identifies many toll fraud vulnerabilities by detecting second dial tones

SCD overcomes many of the limitations of conventional telephone scanning and increases the capabilities of many off-the-shelf modems. It allows faster voice detection and reduces the possibility that redundant calls will be made in the course of a scan. All versions of PhoneSweep include SCD.

Conventional telephone scanning is limited by inflexibilities inherent in modem design. Standard fax/modems can place calls in either “data” mode or in “fax” mode, but cannot place calls in both modes simultaneously. Thus, a conventional scan requires two calls to each number to locate modems and fax machines; all the numbers must be called in data mode to locate modems, and then called again in fax mode to locate fax machines. SCD eliminates the second call to any numbers that are not connected to a device possibly capable of fax communication, thereby reducing the total number of calls in the scan and reducing the time required to complete the scan.

Conventional telephone scanning is also limited by the fact that few modems can reliably identify a human voice answering the phone, and fewer still can detect a second dial tone. Telephone scans that cannot recognize Voice run a high risk of leaving blank voicemail messages and confusing or irritating employees. “Second dial tone” happens when dialing a telephone number results in another dial tone. Detection of second dial tones is essential for detecting unauthorized “telephone extenders” that can be abused to commit toll fraud. SCD detects both by bypassing normal modem synchronization.

2.9.1 How SCD improves scan speed and accuracy

When PhoneSweep in SCD mode is used to perform a telephone scan, the modem and computer listen to and evaluate each call as it is being made, and modifies calling behavior accordingly. If PhoneSweep detects:

- A live or recorded human voice, it immediately hangs up and marks the number as “VOICE.”
- A second dial tone, it hangs up and marks the number as “TONE.”
- A Busy signal, it hangs up and marks the number as “BUSY.”
- Ringing when the call timeout occurs, it hangs up and marks the number as “TIMEOUT.”

Except for those flagged "BUSY", these numbers will not be called again.

Two calls are made to lines to that generate fax and/or modem tones: If PhoneSweep hears tones from a modem, it automatically switches the calling modem into fax mode to determine whether a fax-capable device produced the tones. PhoneSweep then schedules a second call to the same number in data mode to determine if the answering device is also capable of data communications.

SCD speeds telephone scanning in two ways:

- Reduces the time necessary to detect voice responses and second dial tones.
- Reduces the total number of calls PhoneSweep has to make in order to accurately identify data and fax devices (Voice lines and second dial-tone lines are not called back a second time).

With SCD, the dialing modem quickly identifies the response and terminates. **Note:** Numbers that PhoneSweep identifies as voice, second dial tone, or timeout will not be called again in fax mode, as they would be in the course of a conventional telephone scan.

2.9.2 Many off-the-shelf modems support SCD

SCD works with many popular modems. In general, most, but not all, modems with a Rockwell/ Conexant chipset support SCD.

To determine if a particular modem supports SCD, you can use the program *checkmodems.exe*, which is available on the PhoneSweep CD-ROM and downloadable from Sandstorm's web site (http://www.sandstorm.net). Sandstorm also maintains an updated list of modems that work with SCD and modems that are known not to work well with SCD at http://www.sandstorm.net/support/phonesweep/recmodems.shtml.

If you use PhoneSweep to identify both fax and data devices with a modem that does not support SCD, PhoneSweep will automatically place two phone calls to each number in the profile to distinguish among data modems, fax modems, and fax machines. If you use a multiple modem version of PhoneSweep with a mix of different modems that do and do not support SCD, your results will vary based on which modem was used to place a specific call. Sandstorm does not recommend using a mix of SCD and non-SCD modems when sweeping.

2.9.3 Modems that do not support SCD

Please note that as of July 2002, modems manufactured by these companies or that fall into these categories do **not** support SCD:

- 3Com
- IBM
- Lucent
- USRobotics (USR modems other than the Courier Imodem have a bad performance record with PhoneSweep and are strongly not recommended).
- Any modem that is called a "WinModem", or claims to use "HSP" or "HST".
- Internal modems included with your Laptop or Desktop (most turn out to be WinModems). We strongly recommend that you avoid internal modems.
- ISDN-capable modems

The contents of the above list may change, because modem manufacturers may change chipsets, introduce new models, and phase out old models. Please visit Sandstorm's web site at http://www.sandstorm.net/support/phonesweep/recmodems.shtml to get an updated list of modems that support SCD before purchasing a modem to use with PhoneSweep.

Sandstorm is a reseller for some modems that work well with PhoneSweep in the U.S. See **Section 3.7** for more information about modems and SCD.

2.10 Controlling when phone numbers are called

There are times at which it would not be appropriate to call some phone numbers in the course of a PhoneSweep scan. PhoneSweep allows you to control when phone numbers are dialed by specifying:

- The days and times to call each number contained in a given profile (*time periods*)
- Specify **Blackout** hours within or crossing time periods when PhoneSweep should not dial phone numbers assigned to given time period(s).
- How long PhoneSweep will wait for a number to respond (before and after call pickup) before moving on to the next number (**other time-based parameters**)
- **Schedule Start** or **Schedule Stop Sweep** (works only on the currently open profile).

2.10.1 Time Periods

PhoneSweep allows the user to specify that a given phone number should be called in any or all of the three time periods listed below.

Time Period	Default Value
Business Hours	9:00 AM through 4:59 PM, Monday through Friday
Outside Hours	The period of time before and after Business hours on weekdays. PhoneSweep automatically sets Outside hours when the user specifies Business hours.
Weekends	All of Saturday and Sunday (24 hour scanning).

Time periods are generally assigned when you add phone number to the current Profile via the **Phone Numbers** tab or import them via the **Import** button.

You can change PhoneSweep's definition of the three time periods by using the options under the **Setup->Time** sub-tab (see **Setting Time Options** in Section 4.4).

Changing the definition of **Business hours** automatically alters the definition of **Outside hours** (e.g., any weekday hour not included in the new definition of Business hours). For instance, if you want PhoneSweep to scan numbers during Outside hours that run from 10PM to 4AM the next weekday morning, you would set Business hours to run from 4AM to 10PM and assign phone numbers to the Outside hours time period.

You can also determine which days are treated as **Weekend** days by selecting or unselecting individual days on the Weekend list. This allows you to treat Saturday and Sundays as weekdays, subject to Business and Outside hours scanning times; as well as to treat holidays that fall on normal weekdays as weekend days where PhoneSweep can scan a full 24 hours.

2.10.2 Using time periods to control the start of a scan

You can use time periods to begin a scan automatically at a particular time. For example, say you wanted to begin a sweep at 5:00 PM, but you had to leave work early and couldn't be around to start the sweep. Assuming that you had not changed the default time period settings (Business hours: 9 AM to 5 PM), you could create a profile in which all the numbers are only dialed during Outside hours (based on default business hours, start at 5pm), then click on the **Start** button to start the sweep before you left.

PhoneSweep will not dial any numbers until Outside hours begin at 5:00 PM (You will see the green radar going on the bottom right hand side of the user interface even when no numbers are being dialed).

2.10.3 The Blackout period

To exclude specific periods from PhoneSweep's dialing without changing the time period settings, you can use **Blackout Start** and **Blackout End** under the **Setup->Time** sub-tab. For example, one day you may need to exclude the period from 8:00 PM until 9:30 AM to avoid calling while the phone switch is being repaired. You would set the Blackout Start to 8 PM and the Blackout End to 9:30 AM.

2.10.4 Controlling Sweeps through the use of other Time Options

The **Setup->Time** and **Setup->Dialing** sub-tabs also allow you to control the following:

- How long PhoneSweep will wait for a response from a number it has dialed before it goes on to the next number within different time periods (**Setup->Time: Seconds** or **Ring Timeout** – altering one, alters the other)
- How long PhoneSweep will wait for a response after a line picks up (**Setup->Dialing: Single Call Voice Timeout (secs)**.
- How long to wait between calls before dialing (**Setup->Time: Delay between Calls)**. Defaults to 5 seconds. We recommend you do not lower this value, as doing so does not give the dialing modems time enough to set up for the next call.

2.10.5 Schedule Sweep Start and Stop on the currently open profile

As of PhoneSweep 3.0, you can schedule when sweeps on the current open profile will start and stop. The default value is **–OFF--**, as seen in the Start and Stop Sweep boxes at the bottom of the PhoneSweep user interface.

To schedule a start time, click on and hold down the **Start** button until a pop-up menu appears, or select Schedule start from the **File->Start** drop down menu.

To schedule a stop time, click on and hold down either the **Start** button when no sweep is running, or the **Stop** button when a sweep is running, or select Schedule stop from the **File->Start** or **File->Stop** drop down menus. Please see Section 5.4 "**Starting and Ending a Sweep Automatically**" for further information.

2.11 The phonesweep.ini File

Advanced users can use the *phonesweep.ini* file, located in the top-level PhoneSweep directory, to customize PhoneSweep defaults. For example, if you must dial a certain prefix before every phone number in every profile, you can modify the *phonesweep.ini* file to include this prefix by default in every new profile. A more detailed discussion of the *phonesweep.ini* file is found in Section 11, **Customizing PS Defaults Using the PhoneSweep.INI file.**

2.12 Emergency Number Screening

It is highly inappropriate to call local emergency services during a PhoneSweep scan. For this reason, PhoneSweep can automatically screen numbers in an attempt to avoid accidental calls to the emergency number 911 or even 9911. However, there are other emergency numbers or hot lines that you might want to avoid scanning, and outside the United States, emergency numbers other than 911 are used. In PhoneSweep, you can set your own emergency number screening list on a per-profile basis on the **Setup->Dialing** sub-tab. For your convenience, 911 and 9911 are automatically listed.

Sandstorm does **not** warrant that the emergency number screening feature will block all attempted calls to emergency numbers in your area. PhoneSweep will not attempt to automatically block calls to emergency numbers other than those listed in the emergency number screening list. ***It is your responsibility to be aware of the emergency numbers in your area,*** and to block them or avoid including these numbers when creating lists of phone numbers for PhoneSweep to dial. If you are outside the United States or Canada, please be aware of your local emergency numbers and take care not to include them during a PhoneSweep scan.

Emergency number screening is controlled on the **Setup->Dialing** sub-tab. It is strongly suggested that screening 911 and 9111 be left on the emergency number screening list and enabled in the US and Canada.

2.13 Possible Testing Injuries

Scanning phone numbers with PhoneSweep can create undesired results. These results are collectively known as "testing injuries." Accepting the possibility that testing injuries may occur as a result of using PhoneSweep is part of accepting the PhoneSweep license agreement. Happily, if you are aware of the possible testing injuries that can result from using PhoneSweep and how to prevent them, you can generally avoid them. Use of SCD can also reduce the risk of certain testing injuries.

Possible testing injuries include, but are not limited to:

- **Calling local emergency services**. PhoneSweep attempts to block (not place calls to) the emergency number 911 and other emergency numbers specified by you on the emergency number screening list for each profile. Be aware of emergency numbers in the area where you are scanning, and do not include these numbers in dialing profiles. Emergency number screening can be disabled, but Sandstorm strongly recommends that it be left enabled in North American environments.
- **Calling human-answered phones in fax mode**. Scanning for fax machines requires an audible beeping. If PhoneSweep is scanning in fax mode, people who answer the call will be aware that a telephony device has called them. If your users don't know that PhoneSweep is being used to conduct a security audit, this may cause complaints. Users aware of security issues and procedures may be concerned that they are being "war dialed" by an outsider. This testing injury is largely avoided with SCD, because when SCD hears a voice answering a call, no fax tones are sent.
- **Calling human-answered phones while scanning for ISDN-capable devices**. Some ISDN-capable devices produce a loud, audible beep when calling a voice line. We suggest you only scan for ISDN-capable devices when there is a low probability of a human answering the call. PhoneSweep cannot prevent this testing injury because to date, no ISDN modems support SCD.
- **Repeatedly calling a single location after business hours**. In some organizations, all calls may route to a single central point, such as a security desk, after business hours. This is sometimes referred to as "Night Service". PhoneSweep will only generate useful results when night service is not in effect, or is switched off for the duration of the scan.
- **Inadvertently making a phone call while testing COM ports**. To test COM ports, PhoneSweep employs a helper program, *checkmodems.exe*. *Checkmodems.exe* dials the digits "55" in order to test a COM port. If your local PBX (private branch exchange) is configured so "55" is a valid number, *checkmodems.exe* should not be run while any modems are connected to the telephone switch.
- **Leaving blank voicemail messages.** If a voicemail system answers, PhoneSweep may not automatically hang up before a message is recorded. If this occurs, PhoneSweep can usually be

configured to terminate calls before your voicemail system answers. Be aware that if your modem does not support remote ring detection (that is, if it doesn't report each time the remote phone rings) only the seconds-based timeout will be used. You should set the seconds-based timeout to be equivalent to the correct number of rings. This testing injury is less likely if you are using SCD. If you are using SCD, PhoneSweep will hang up as soon as it detects the recorded voicemail prompt, and this normally prevents a blank voicemail message.

In the event that SCD does leave a blank voicemail message, try lowering the “Single Call Voice Time Out” option to 4 or 3 seconds. Or try to find out if your Phone System can be altered to not take voice mail messages if a call hangs up in time. Contact your vendor to determine if they can supply patches that allow this. If that does not work, contact support at Sandstorm Enterprises, Inc.

3 Installation and Setup

This section guides you through the process of getting ready to run PhoneSweep. To successfully install and begin using PhoneSweep, you must:

- Have TCP/IP, Winsock 2 and HTML help installed on your computer.
- Select appropriate modems for your computer.

3.1 System Requirements

3.1.1 Dialing Computer

If PhoneSweep will be in continuous operation or will be mission critical, we recommend that you install PhoneSweep on a well-maintained PC with up-to-date software (e.g. relevant service packs installed and latest drivers). Also, both the PC and PhoneSweep should be tested well before you use PhoneSweep on an actual sweep. [This is especially true where the intended system has previously had problems with other software, or you intend to use PhoneSweep at multiple locations and conditions.]

Basic requirements for all versions of PhoneSweep include:

- **Turn off all virus Checkers, Power Savers and Screen Savers during PhoneSweep operation**, as they can interfere with PhoneSweep's operation, causing it to freeze. (In some cases, you may find that you can use PhoneSweep with your Screen Saver. If your system freezes during a scan, then turn the Screen Saver off).
- Remove other Wardialing or modem-based software if you find PhoneSweep cannot access the COM ports used by your modems. (At least one commercial grade Wardialer is known to hang on to the COM port resources even when shut down). Reboot if you find you cannot reach the Modem COM ports after using HyperTerminal.
- **If you need Password and/or Screen protection**, try ScreenLock found at http://www.screenlock.com.
- **You can use a local Firewall with PhoneSweep** (Please see the section below on Firewalls and TCP/IP).
- **Microsoft Excel 2000 or greater version** – to use **Chart** feature.
- **Microsoft Word** to view PhoneSweep reports (RTF format).
- **Winsock 2** and **HTML Help**: Please see Section "Winsock 2 and HTML Help" below.

Minimum requirements: **For 1 modem (PS Basic), with small profiles**: 200 MHz PC or laptop, with 32MB RAM, Intel Celeron/PII, and 50MB of free space to store the PhoneSweep program and the profiles you create.

To use Single Call Detect, bruteforce PPP systems, or 4 modems (PS Plus), Sandstorm recommends using a 400 MHz or faster processor.

Optimal requirements: **For 8 modems (PS Plus 8), and/or large profiles**: 333 MHz PC or laptop, with 64 MB RAM, Celeron/PII or Pentium III, and 100 MB of free space to store the PhoneSweep program and profiles you create.

To use profiles over 10,000 numbers (above our supported level of operation), Sandstorm recommends using a 400 MHz or faster processor.

Of course, the more data you need to store, the more disk space you will need. If you are using PhoneSweep with four or more modems, you will also need appropriate hardware to connect the modems to your computer. (See section "Modem and multi-port serial I/O hardware recommendations" below).

Additional Minimum System Requirements: **For PhoneSweep Plus 12 or 16:** 600-700 MHz Pentium III or equivalent and 128 MB of RAM

If you have profiles over 20,000 numbers (i.e., above our supported level of operation) Sandstorm recommends using 256 MB RAM.

3.1.2 Operating System

PhoneSweep is certified to run under Microsoft Windows 95, 98, NT 4.0, XP, and Windows 2000 Professional SP2 and Windows 2000 Server SP1. We do not recommend or support using PhoneSweep on Windows ME. If you have a choice of platforms, we recommend that you install PhoneSweep on a computer using **Windows 98 or Windows 2000**, as these are the two most stable platforms we have found to date. PhoneSweep works on both FAT and NTFS file systems.

3.1.3 A cautionary note on laptop computers and Windows NT

Sandstorm has noted that PhoneSweep has historically had more problems running on laptops with Windows NT than on laptops running Windows 95/98, especially with laptops equipped with multi-port serial cards. Sandstorm supports NT platforms, but recommends that, if possible, users who wish to run PhoneSweep on a laptop computer use Windows 98 or Windows 2000 for the operating system.

3.1.4 Modem and multi-port serial I/O hardware recommendations

Please see the "Recommended Modems" and "Multi-port Card" sections of this manual or follow the links on our main website (http://www.sandstorm.net) for the most up-to-date information. If you are using more than one modem, you must use a multi-port serial I/O card.

Our most recommended analog modem is the Zoltrix External Rainbow 56K modem, which we can provide within the U.S. and is sold worldwide. Other modems that we recommend are the Multi-Tech MultiModem MT5600 ZDXV, and EXP Computers ThinFax 56L (model # MF-PCA56-L), which are also sold worldwide.

For PhoneSweep Plus 12 and Plus 16, we recommend that you use the Multi-Tech Multimodem MT5600 ZDXV (see below for further details). For ISDN scanning we recommend the U.S. Robotics Courier Imodem.

For PhoneSweep Plus and Plus 8, the multi-port serial I/O cards we recommend most are Sea Level's Versa COMM +4 or +8 Serial I/O PCI cards for PCs and Quatech's QSP 100 PCMCIA cards for laptops (Each QSP 100 supports up to 4 modems, so you must use two cards for PhoneSweep Plus 8).

Windows NT users please note: Windows NT does not support the use of multiple multi-port serial I/O cards, which limits Windows NT Laptops to using only one QSP 100 PCMCIA card and Desktops to using only one SeaLevel Versa COMM +8.

Windows 2000 users please note: If installing a SeaLevel device that you have owned for more than 6 months on Windows 2000, make sure that you have obtained the latest drivers from SeaLevel's website, which may not be on your install CD. Some old SeaLevel drivers (Pre-Jan 2001) will cause your system to freeze or not work properly.

For PhoneSweep Plus 12 and 16 (Desk tops only), we recommend the use of:

- Multi-Tech ZDX Modem Rack (http://www.multitech.com) which takes up to 12 Multi-Tech MT5600ZDXV modems. (For PhoneSweep Plus 16, you would need to place 4 standard Multi-tech MT5600ZDXV modems to the side).
- Digi AccelePort 16em (http://www.digi.com) multi-port, which provides 16 serial I/O ports for your desktop, connecting through a PCI card.

3.1.5 Modem Phone Line(s)

Modem Phone Line(s) should be dedicated analog or ISDN phone lines, free of incoming calls. Incoming calls will cause line errors and interfere with PhoneSweep's operation (PhoneSweep will stop dialing on that line). If dialing outside your local phone system, we recommend using direct lines if possible. Please verify that each line is free of blocks on both your side and telephone company's side.

3.1.6 Security

We recommend for added security, that the PhoneSweep system not be connected to any network; or that you disconnect the system from the network when you are not present. If system is on a network, such as when using Gold Distributed and/or Automatic E-mail Notification options, all security precautions should to be followed (See your Network/Systems Administrator and the PhoneSweep Gold Manual for additional information). You can also place a Firewall on the same machine as PhoneSweep. For proper set up, please see section "***Firewalls and TCP/IP"*** below.

3.2 TCP/IP

TCP/IP must be installed on your computer in order for PhoneSweep to install and function correctly. PhoneSweep uses TCP/IP to communicate locally among the engine, user interface, and SQL database. This means that your desktop or laptop computer should on some level be network capable, even if you never attach it to a network.

Specifically, a TCP/IP protocol stack must be installed on your computer. This is rarely an issue with Windows 98. If your computer is on a network, the TCP/IP protocol is probably already installed. If it isn't installed, you can install one by selecting "Network" in the Control Panel, then "Configure", then "Add", then "Adapter", then "Microsoft", then "Dial-Up Adapter". An installed dialup adapter is sufficient to run PhoneSweep **(except under Windows 95A; see the following paragraph).** The computer running PhoneSweep does not need to be actually connected to a network. If the TCP/IP protocol is only loaded under certain configurations (such as DHCP), PhoneSweep will only run when it is loaded. Sandstorm's website has a support PhoneSweep FAQ which contains a section on how to set up TCP/IP properly on your computer.

Additionally, some software can interfere with PhoneSweep's operation over TCP/IP, as can misconfigured Firewalls on your local machine. (Please see our sections "Firewalls and TCP/IP" and "Software that can interfere with PhoneSweep operation.")

3.2.1 Issues with Windows 95A

If you are using an early version of Windows 95 called Windows 95A, TCP/IP is only loaded, and PhoneSweep will only run, when the computer is connected to an IP network. PhoneSweep ships with a patch that will correct this problem. To upgrade the Windows TCP/IP software under Windows 95A, run the *msdun13.exe* file found in the top-level PhoneSweep directory.

If you are not sure which version of Windows 95 is installed, right click on the “My Computer” icon on the Windows desktop. Select the “Properties” option, and look under the “General” tab. On the upper right-hand quadrant of the tab, underneath the “Windows 95” line, is the version number. If the version number is 4.00.950 A, Windows 95A is installed, and you should run the *msdun13.exe* patch if the machine running PhoneSweep does not have a full-time network connection. Otherwise, you don't need to install the patch.

3.2.2 Firewalls and TCP/IP

You can use Firewalls on your local desktop or laptop computer, provided the following:

- Allow Port 4321 for standard PhoneSweep operations on your local computer.
- Allow Port 4322 for PhoneSweep Gold Distributed and other remote operations, otherwise keep this port closed.

If you allow connections based on programs (such as can be set in Zone Alarm) you must allow the following:

- Phonesweep.exe
- MySQLD.exe (PhoneSweep MySQL database)
- PS.exe (PhoneSweep user interface)
- PhoneSweep Engine
- MySQLD-OPT.exe
- Other utilities as needed (Debug.bat, isamchk.exe, brutecreate.exe, etc.)

3.2.3 Software that can interfere with TCP/IP operation

Some network software, or other programs that use TCP/IP have been known to interfere with PhoneSweep’s operation. If you find PhoneSweep is unable to operate over TCP/IP, try using PhoneSweep on a machine that does not have the same network software, or, if possible, removing the network or other software from the current machine.

3.3 Winsock 2 and HTML Help

PhoneSweep requires WinSock 2.0 and HTML Help in order to function correctly. The installer will attempt to detect whether either needs to be installed, and will try to start the appropriate Microsoft installation program if so. If you are missing these programs, installers for each are included on the PhoneSweep distribution CD:

- ***hhupd.exe*** is the HTML help installer. This is already installed if you have Internet Explorer 4.01. If you don't have Internet Explorer 4.01 or later, you will need to run *hhupd.exe* from the PhoneSweep installation CD before PhoneSweep online help will work. We recommend that you run this program before installing WinSock 2.0.
- ***w95ws2setup.exe*** will install WinSock 2.0 on your system.

3.4 Preparing to install and run PhoneSweep

Before you install, reinstall, upgrade, or run PhoneSweep, prepare your computer by following these steps:

- **If you are installing PhoneSweep Plus 4,Plus 8, 12 or 16 for the first time,** we recommend that you install multi-port cards with their respective COM ports before installing PhoneSweep. Make sure that your PC can see the COM ports. This helps to separate hardware install problems from PhoneSweep problems. (Note SeaLevel cards require you install the drivers before the hardware).
- **Disable your PC's power management software**. Because of bugs in some power management drivers, computers with power management active may occasionally enter "sleep" mode while PhoneSweep is running.
- **Disable your PC's fax software**. Most fax software cannot share COM ports with PhoneSweep.
- **Disable your PC's screen saver**. Some screen savers require a substantial amount of computational power in order to run. Others place the computer into "sleep" mode, even if power management is disabled. In order to minimize any possibility of conflict, we recommend that all screen savers be disabled before installing or running PhoneSweep. If your screensaver does interfere with PhoneSweep's operation and you need to lock or password protect your screen we recommend using **Screen Lock**. It works on Windows 95, 98, and NT 4.0 and allows you to run PhoneSweep and other programs in the background. You can obtain it from http://www.screenlock.com.
- **Clear your PC's outgoing phone line**. PhoneSweep may encounter problems sharing a local phone line with other functions. Lines with voicemail configured may confuse a modem, preventing it from detecting a dial tone. Fax machines on the same phone line as PhoneSweep may respond to outgoing fax calls. This may lead PhoneSweep to conclude that all numbers it dials reach fax machines.
- **Unplug your PC from your local area network**. We recommend that all computers running PhoneSweep be disconnected from local area networks and from the Internet. This recommendation does not have to do with PhoneSweep itself; it stems from the fact that the computer running PhoneSweep may contain a significant amount of sensitive information. Unplugging your computer from the local area network is one step you can take to ensure that this computer is not compromised. If you must have your PC on a network, please speak with your Systems administrator and follow these guidelines:
  - Do not run a firewall on your PC during PhoneSweep's operation as it can interfere with PhoneSweep.
  - Do not allow your IT department to update software on your system during PhoneSweep operation, as it can cause PhoneSweep to freeze.
- **Log in using an administrator account (Windows NT only)**. On Windows NT series machines, PhoneSweep installs a service to handle communications with the hardware license manager. If an administrator does not install PhoneSweep, the installation process will fail.
- **If you are running Windows NT, attach the hardware license management device (the "dongle") to the computer's parallel or USB port**. PhoneSweep will not install correctly on NT systems if the dongle is not attached during the installation. After installation, PhoneSweep will not make calls from *any* systems without the dongle being attached.

3.5 Installing PhoneSweep

Note that you cannot reinstall or upgrade PhoneSweep while the program or any parts thereof are running. If an attempted installation results in an error message indicating that parts of PhoneSweep are still running, you can use the Task Manager (accessed by simultaneously pressing CTRL-ALT-DELETE) to kill the parts of PhoneSweep that are still running, including MySQLd, or reboot your computer.

Insert the PhoneSweep CD-ROM into your CD-ROM drive. PhoneSweep is distributed as an industry-standard InstallShield package to ease the installation and removal process. If you have not disabled Autorun, the installer will start up automatically after the drive closes. If the installer does not start automatically, select Start and then Run from the Windows startup menu, and use Browse to locate and run the program *setup.exe*. In either case, a standard InstallShield installer will guide you through the installation process. You will not need to place the PhoneSweep CD-ROM in the drive to run PhoneSweep after it is installed.

PhoneSweep's default installation is: C:/Program files/Sandstorm/PhoneSweep.

If you have problems installing PhoneSweep, please consult Appendix C: PhoneSweep Troubleshooting Guide.

3.6 Hardware License Protection

PhoneSweep is a powerful program that can uncover many weaknesses in a telephone system. This information could potentially be very damaging if misused. It is important that PhoneSweep only be used by those authorized to do so. Therefore, to help ensure that unauthorized persons do not use PhoneSweep, a **hardware license manager device (also called a "dongle") is shipped with PhoneSweep and must be attached to the computer's parallel or USB port in order for PhoneSweep to function.** PhoneSweep is shipped with a parallel port dongle. Laptop users may want to use the USB dongle. A USB port dongle can be substituted for a small extra charge.

PhoneSweep will not place calls if the dongle is not attached to the computer's appropriate port. This allows you to lock the dongle in a safe place and be assured that, for example, a disgruntled employee cannot use PhoneSweep to collect information about vulnerabilities in your organization's telephone system, or use your telephone resources to sweep another organization.

If you attempt to run PhoneSweep without the dongle attached, it will run in demonstration mode and not make any actual calls. This means that even if an unauthorized person procures a copy of PhoneSweep, that person will be unable to use that copy without the dongle. PhoneSweep will display a warning message if it is started without the dongle in place.

Do not remove the dongle while PhoneSweep is running! PhoneSweep will cease to function properly if the dongle is removed. If the dongle is disconnected while PhoneSweep is running, it will be necessary to shut down PhoneSweep, reattach the dongle, and restart PhoneSweep.

PhoneSweep's standard dongle works with most PC parallel ports, and does not preclude other simultaneous use of the parallel port. (*If you have ordered PhoneSweep with the optional USB dongle, see below for special installation instructions.)* The parallel dongle works with:

- Standard parallel ports
- Bi-directional parallel ports
- ECP ports
- EPP ports
- Most other PC parallel ports

You can attach other devices to your computer's parallel port while the dongle is in place. You can attach peripherals such as a Zip drive, a Visioneer PaperPort, another vendor's dongle, or even a printer. When attaching another device to the same parallel port as a PhoneSweep dongle, connect the dongle directly to the computer and connect the other device to the dongle.

3.6.1 Laptop models known to have problems with the dongle:

Sandstorm has encountered a few hardware-specific problems with the dongle.

- On most Dell laptops, the *external floppy drive can't be used through the dongle*.
- The dongle *does not work with Toshiba Tecra 700* series laptop computers. The problem is limited to the 700 series of Toshiba laptops; the Toshiba Portege 7020 model and other Toshiba laptops are reported to work properly**.**
- On some laptops, the *parallel port may not automatically activate if the laptop is running on battery power*. In this case, a device with its own power supply, such as a printer or fax machine, needs to be plugged into the laptop.

If PhoneSweep is unable to detect the dongle on a laptop, please contact Sandstorm; the USB dongle may suit your circumstances better.

Check **Appendix C: PhoneSweep Troubleshooting Guide** if you have problems with the dongle. After trying the suggestions there, if you are still having problems with the hardware license manager, contact Sandstorm Enterprises technical support at *support@sandstorm.net.*

3.6.2 Software known to interfere with dongles on the parallel port

Some printer drivers may interfere with the dongle. Other software that uses the parallel port may also interfere. A list of specific software that interferes with the dongles on parallel ports will be forth coming on our web site.

3.6.3 Instructions for installing the optional USB dongle

Sandstorm now offers a USB dongle as an alternative to the parallel port dongle for Windows 98 and Windows 2000 systems only. **The USB dongle should be installed before installing the PhoneSweep software.** We recommend the following installation steps for the USB dongle:

1. Insert the PhoneSweep CD in your CD-ROM drive. The USB drivers are on the CD.
2. Plug the dongle into an available USB port.
3. If your system detects the dongle, proceed to step 5.
4. If your system didn't detect the dongle, try rebooting. If it still doesn't detect the dongle, use the Manual Installation steps below.
5. If you are given the option to choose a device type, choose "Other Devices" or "Unknown Device".
6. At the hardware list screen, click on the "Have Disk" button.
7. Select your CD-ROM drive with the PhoneSweep CD in it, as the location of the drivers.
8. Back at the hardware list screen, choose the appropriate USB Dongle selection for your version of Windows.
9. Proceed with the rest of the installation as prompted by Windows.

Manual Installation: If your system was unable to detect the USB dongle, manually install the driver as follows:

10. Plug the dongle into an available USB port.
11. Open the Control Panel. Open the Add New Hardware or Add/Remove Hardware panel, depending on your system.
12. Follow the steps to add a new device. When you are given the option to choose a device type, choose "Other Devices" (Win98) or "Add a new device" (Windows 2000).
13. If Windows asks you to either search or select the hardware from a list, choose to select from a list.
14. At the hardware list screen, click on the "Have Disk" button.
15. Select your CD-ROM drive with the PhoneSweep CD in it, as the location of the drivers.
16. Back at the hardware list screen, choose the appropriate USB Dongle selection for your version of Windows.
17. Proceed with the rest of the installation as prompted by Windows.

3.7 Selecting Modems for use with PhoneSweep

PhoneSweep requires at least one modem in order to scan a set of phone numbers. The quality of the information that PhoneSweep gathers strongly depends on the capabilities and caliber of the modems used with PhoneSweep. Some features of PhoneSweep, such as Single Call Detect, will only work with a sufficiently capable modem:

- Most, but not all, modems with a **Rockwell (or Conexant) V.90 chipset** support SCD. (Note: Conexant bought Rockwell, so some manufacturers now call it the Conexant chipset**.)**
- *Rockwell/Conexant modems that specifically mention support for "Simultaneous Voice and Data" (SVD) will almost always be usable with PhoneSweep Single Call Detect.*
- *Avoid using modems made before 1997*, as they may not have a new enough version of the Rockwell/Conexant chipset, even though checkmodems.exe says they are SCD capable.
- Modems that ***do not have Rockwell/Conexant chipsets will NOT support Single Call Detect and may not work accurately with PhoneSweep.***

Advancing With The Times: New Conexant 3.3v Chipsets and PhoneSweep*:* As of PhoneSweep 3.01, we began testing and approving modems that use Conexant's new 3.3v chipsets for use with PhoneSweep 3.01 and above. With one exception, modems that use the Conexant 3.3v chipset are *not compatible* with earlier versions of PhoneSweep. We have made a special note of these modems in our list on our web site. As of PhoneSweep 4.4, a subset of some V.92 modems are approved for use with PhoneSweep.

A word of caution: If you use less capable modems in combination with more capable ones, your results will vary based on which modem was used to make a particular call. For this reason, we recommend using identical or at least similar modems with PhoneSweep Plus, Plus 8, 12 and 16, and that they all be Single Call Detect-capable. (See the Section **Equipping a Desktop Computer with Multiple Modems**, for multi-port and rack information.)

If you want to use PhoneSweep to scan ISDN devices, please refer to Section 3.9 "Recommended ISDN capable modems". We recommend that you if want to scan both ISDN and Analog modems, you run separate scans over two different modems. *ISDN modems are **not** Single Call Detect capable.*

If you plan to use multiple modems, you must install a Multi-Port Serial I/0 card: Please see

More about Modem capabilities: Some modems can report more information about the results of a call than other modems. The more capable modems can recognize:

- **A second dial tone.** These modems can determine when dialing a telephone number results in the phone emitting a dial tone, as is the case with some telephone access codes. *A modem that is scanning with Single Call Detect will detect second dial tones and report them as "tone".*

- **A phone answered by a human voice,** such as a recorded voicemail message or an actual human being.

- **Remote ringing.** A modem that supports remote ringing will report each time it hears a ring tone while waiting for a remote device to answer. At this point, few modems support remote ringing, and *there are no modems that support both SCD and remote ringing.*

PhoneSweep uses one of two methods for determining how long it should wait before ending a connection, depending on the type of modem being used: "timeout in seconds" or "timeout in rings."

- **Modems that do not use Single Call Detect or report remote ringing** will not be able to determine when a line has picked up, nor will they be able to report if a call results in Voice and Second Dial Tone responses. Non-SCD modems cannot tell the difference between a "TIMEOUT" after a line has picked up and "RING TIMEOUT" when the line never picks up. In these cases, PhoneSweep must rely on a **"timeout in seconds**" to end a connection. *Calls that SCD would answer as voice, a second dial tone, or do not pick up will all be reported as timeouts.*

- **Modems that use Single Call Detect (but are not capable of remote ring detection)** will correctly report voice and second dial tone responses; however, *for lines that do not pick up from ringing, PhoneSweep must still rely on a timeout in seconds to end a connection that never picks up. After call pickup, PhoneSweep uses "Single Call Detect Voice Timeout" to determine how long to wait for a response (Voice, Tone, Fax or Modem) before reporting it as a timeout.*

- **Modems that support remote ring (but not Single Call Detect)** will rely on the *timeout in rings* to determine when to report a "RING-TIMEOUT." As with other non-SCD capable devices, voice and second dial tone responses will be reported as timeouts.

In general, **Sandstorm recommends that you use external modems with PhoneSweep,** rather than internal modems. External modems are generally more configurable than internal modems, especially, with regard to which IRQ their COM port uses. It is easier to diagnose problems with external modems, and they are easier to replace if they fail.

Many internal modems are software-based win-modems*, such as ACP modems that come with IBM ThinkPads. Even if they do work with PhoneSweep, you will not be able use Single Call Detect with these modems, and you may have to turn off Single Call Detect in order to get any accurate results.

You do not have to install the modem drivers for a modem to work with PhoneSweep.

3.8 Recommended Modems

The specific modems that Sandstorm Enterprises recommends as of July 2002 are listed below. All these modems have been tested by Sandstorm and support Single Call Detect. Sandstorm Enterprises is a reseller for some SCD-capable modems within the U.S., Check the Sandstorm website (http://www.sandstorm.net/support/phonesweep/recmodems.shtml) for current information.

Most modems on this list are manufactured worldwide, obtainable through Manufacturer's local representative or through resellers.

Please note the specific models of the modems listed below. *The fact that one modem by a specific manufacturer supports SCD does not guarantee that other modems made by that manufacturer supports SCD.*

- **Zoltrix External Rainbow Modems, FM-VSP56e2 and FM-VSP56e3:** The Zoltrix modems are high-performance fax/data modems. To find a local retailer for your country, go to bottom of the *Zoltrix International About Us* web-page http://www.zoltrix.com, map. These modems have a female DB9 connector on the back and come with a serial cable for easy installation. If you are unable to find Zoltrix Modems in the USA, Sandstorm sells the FM-VSP56e3 Rainbow modem. The general Zoltrix product index can be found at http://www.zoltrix-int.com/products/modem/modem.htm, where the Zoltrix External Rainbow Modem is listed.

- **Zoltrix External Raptor 56K, Model 8FM-56KRAPTOR:** This modem is supported as of PhoneSweep 4.4, and uses a newer chipset version than the Zoltrix Rainbow.

- **AOpen External Box Modem FM56-EX:** (http://www.aopen.com) This is a high-performance modem that is shipped with a serial cable for easy installation. Newer versions of AOpen modems are not all compatible with Single Call Detect, check the model number carefully before you buy.

- **Multi-Tech systems MultiModem 56K Voice/Data/Fax,** Multi-Tech MT5600ZDX and MT5600ZDXV: (http://www.multitech.com) These modems are rack mountable on Multi-Tech's 12 modem Rack Mounts. (Please see "Equipping a Desktop Computer with Multiple Modems" for further information. **Note:** These modems do not come with a serial cable, which must be purchased separately. Sandstorm does not recommend other Multi-Tech modem models for use with PhoneSweep, as they do not support Single Call Detect.

- **EXP Computers ThinFax 56L Model # MF-PCA56-L:** (http://www.expnet.com) Low Power PCMCIA card for laptops, featuring Rockwell/Conexant's 3.3v chipset technology (the only 3.3v chipset that works with all versions of PhoneSweep**)**.

- **Diamond SupraExpress 56i Sp, 56K internal ISA Modem & Speakerphone** (http://www.supra.com) Approved for use with PhoneSweep Basic only, as most machines do not have 4 open ports.

3.8.1 3.3v chipset Modems approved for PhoneSweep 3.01 and above

The three 3.3v modems below are only approved for use with PhoneSweep 3.01 and above:

- **Best Data Smart One Serial External 56K, Model #DI5601:** (http://www.bestdata.com) Low Power external modem, featuring Rockwell/Conexant's 3.3v chipset technology.

- **Best Data Smart One USB external 56K, Model #56USB.** (http://www.bestdata.com). **Windows 95 and 98 only.** USB modem, featuring Rockwell/Conexant's 3.3v chipset technology.

- **Creative Modem Blaster 56K internal ISA, Model #56SX. (**http://www.bestdata.com). Internal ISA modem, featuring Rockwell/Conexant's 3.3v chipset technology.

3.8.2 Other modems tested by Sandstorm

Sandstorm is constantly testing new modems to find those that work best with PhoneSweep. For an up-to-date list of the modems Sandstorm has tested and our recommendations, please see http://www.sandstorm.net/support/phonesweep/modemtests.shtml. Also, please feel free to contact Sandstorm Enterprises to discuss modem-related issues and your particular needs.

3.8.3 Modems Not Recommended

Sandstorm Enterprises specifically **recommends against the use of almost all US Robotics modems** for telephone scanning. Although these modems are well suited to "normal" data connections, their voice detection attempts have caused several problems with some PBXs and voicemail systems.

Sandstorm Enterprises also specifically **recommends against the use of PhoneSweep with "WinModems", such as ACP modems (Most internal laptop modems seem to be WinModems).** These modems work mostly in software, and do not interoperate correctly with PhoneSweep. *Some of these modems may even crash your computer if you use them with PhoneSweep.*

3.8.4 Modems recommended by customers in other countries

Below is a table of Single Call Detect capable modems recommended by customers in other countries. Note that we have not been able to test these modems ourselves. Please see the section on initialization strings for additional information on using modems outside the United States. Let us know about any Single Call Detect capable modems that should be added to this list.

Please note: Since customers initially recommended the Elsa Microlink 56K modem for use in Austria, England, Germany and Sweden, we have seen Elsa become a Global manufacturer.

We have tested the US model of the Elsa Microlink 56K modem and find it does not work with PhoneSweep (does not seem to recognize USA dial tone), so, outside of Europe, we recommend that customers who try the Elsa Microlink 56K modem do so only if you can return it for not being compatible with PhoneSweep.

Not recommended: Dynamode, used in Israel. While it is made by the same manufacturer as the Dynalink (Askey Computers), it is not Single Call Detect capable.

Country	Modems	Notes
Australia/ New Zealand	Dynalink V1456VQE.	Available through PC suppliers all over Australia. Online suppliers easily found on Web searches for the modem. http://dynalink.com.au
Australia/ New Zealand	NetComm 56k V.90	Sirius puts out several modem brands. Online suppliers easily found on Web searches for the modem. http://www.sirius.com.au

Australia/ New Zealand	Lightfax 56k V90	We have some reservations about this modem, as we have only found the manufacturer's home page, and only two online retailers. http://www.wyntec.com.au/modem.htm http://www.pcsol.com.au/modems.htm
Sweden, Austria, Germany,	ELSA Microlink 56K Office	This modem is being used successfully in Sweden and Austria to sweep Analog lines on Hybrid ISDN/Analog PBXs. http://www.elsa.com
Germany	ELSA ISDN/TLV34	This is being used to sweep ISDN lines on a Hybrid ISDN/Analog PBX in Germany. http://www.elsa.com

3.9 Recommended ISDN-capable modems

Sandstorm recommends the **US Robotics *External Courier Imodem* for scans involving ISDN devices, both domestically and outside the U.S.** This is the one exception to Sandstorm's recommendation that USRobotics modems not be used with PhoneSweep. The *Imodem* is a hybrid modem that can find analog and most ISDN modems. Note that the *Imodem* does not support Single Call Detect.

We recommend that if you wish to both find ISDN devices and scan in SCD mode, that you scan the profile twice, once with an SCD-capable modem and again in data-only mode ("Find Modems Only" or "Find Fax Only") with an ISDN-capable modem.

You can use a hybrid analog/ISDN modem to perform all the calls, but because you lose the Single Call Detect functionality, the scan will make approximately twice as many calls. Also, using a hybrid analog/ISDN modem for every call will impact users more because it lacks rapid voice ID, so a human answering the phone will be subjected to extremely loud beeping.

3.9.1 ISDN sweeps in foreign countries

A customer in Germany with problems while sweeping ISDN lines on a Hybrid ISDN/Analog PBX found they were able to use the US Robotics Courier for sweeping ISDN lines.

In Germany, we have one customer who has reported using the ELSA ISDN/TLV34 to sweep ISDN lines on an ISDN/Analog Hybrid PBX with some success. We are unable to test this, because to date, ELSA does not produce U.S. versions of their modems. We can only recommend that you try this modem if you can return if it does not meet your needs.

3.10 Scanning in Multiple Countries

For scanning in multiple countries, please be aware that you may not be able to use your modem in multiple regions of the world. Like power standards, modem and phone system standards vary from region to region. Not only do you need a proper power adaptor for each region, but you also need a modem configured for the local modem and phone standards. Only a handful of modem manufacturers build modems that you can reconfigure for different regions with software that they supply.

Sandstorm will be investigating which modems can be best used in multiple regions over the next few months. This information will be placed on our web site and in the next version of the PhoneSweep Manual. If you do plan to scan in multiple countries with a laptop, you may wish to speak with a

manufacturer who specializes in manufacturing modem and power adaptors for mobile devices. Teleadapt is one such company: http://www.teleadapt.com.

3.11 Testing COM ports, Modems using checkmodems.exe

Checkmodems.exe can be found in the PhoneSweep directory. Because PhoneSweep controls each modem directly, PhoneSweep can use COM ports from COM 4 up to and including COM 255. *Checkmodems.exe* can scan all COM ports from 1 to 255. It can also be used to check specific ports.

After installing your Modems and any required Serial I/O port adaptors into your PC or laptop, and before you run PhoneSweep for the first time, run *checkmodems.exe* to verify that COM ports are reachable (Usually Windows assigns COM ports 5 through 8 for 4 port cards and COM ports 5-12 for 8 port cards).

- verify what COM ports your modems are on
- verify that modems attached to your computer are in good working order
- detect modems that support SCD

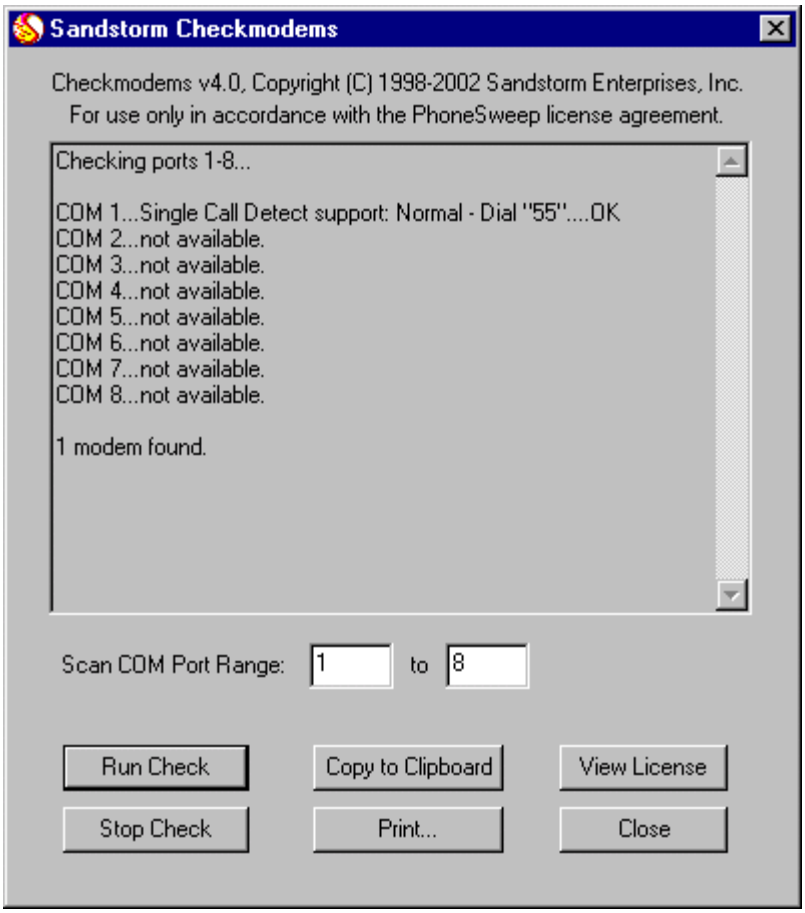
To test **all COM ports**, do one of the following:

- As a DOS line command: Open a MS-DOS prompt window and go to the PhoneSweep directory. At the DOS command prompt, type: `checkmodems.exe <Return or Enter>`
- Double click the *checkmodems.exe* icon in Windows Explorer
- Select the "Check Local Modems" option from the PhoneSweep category of the Start->Programs Menu.

If there is no hardware installed for a given COM port, or if another application is using it, *checkmodems.exe* will fail to open the COM port.

If *checkmodems.exe* successfully opens a COM port, it then tries to turn on the speaker of a modem connected to it and determine if it is attached to an active, working phone line. If a dial tone is detected, *checkmodems.exe* then attempts to dial "55" on that port.

C*heckmodems.exe* displays its findings for each active COM port as it scans. For example:



If *checkmodems.exe* finds the modems, but PhoneSweep says it can't find the COM ports, please verify which COM ports *checkmodems.exe* reports finding modems on, then go to the PhoneSweep options **Setup->Modems** sub-tab. If your modems are not set to the same COM ports that *checkmodems.exe* reports, you can change the COM ports by clicking on the drop down menu in the COM port column next to each modem.

3.12 Configuring your PC to support 4 or more Modems

Most Windows-based PCs today are delivered with one or two serial ports, COM1: and COM2:. The Windows operating system allows up to four serial ports to be addressed through the standard COM port serial driver. Unfortunately, the task of actually getting a standard PC to recognize 4 or more serial ports is complicated by history and hardware limitations.

3.12.1 IRQs and I/O addresses

Personal computers have grown more complicated in recent years. Today's laptops and desktops are equipped with sound cards, Ethernet cards, infrared interfaces, and more. Unfortunately the PC's IRQ (interrupt request) system still offers only 16 IRQs. Fortunately, a variety of techniques have been developed to "share" IRQs between multiple devices. Newer PCI-based interface cards can "share" a single IRQ, but older 8-bit and 16-bit cards that use the ISA bus cannot share IRQs.

If you are running the Windows 95/98 operating system, you can easily generate a list of the IRQ and I/O Address assignments on your computer:

- Right click on the "My Computer" desktop icon.
- Click the "Properties" menu.
- Click on the "Device Manger" tab of the "Systems Properties" window.
- Double-click on the word "Computer."

This will show your computer's IRQ assignments. The table below shows the IRQ and I/O Address assignment for a new laptop computer running the Windows 98 operating system. This computer has one serial port (COM1) and one parallel port (LPT1).

TYPICAL LAPTOP/WINDOWS 98 CONFIGURATION		
IRQ	**I/O Address**	**Device**
0	0040 – 0043	System Timer
1	0060 - 006F	Standard 101/102-Key or Microsoft Natural Keyboard
2		Programmable interrupt controller
3		
4	03F8 - 03FF	K56Flex HSP PNP Modem (COM1:)
5	0220 - 022F 0388 - 038B	Crystal PnP Audio System CODEC
6	03F0 - 03F7	Standard Floppy Disk Controller
7	0378 - 37F	Printer Port LPT1
8		System CMOS/real time clock
9	02F8 - 02FF	SHARP Fast Infrared Adapter
10		IRQ Holder for PCI Steering
11		Ricoh RL5C475 CardBus Controller
12		PS/2 Compatible Mouse Port
13	00F0 - 00FF	Numeric data processor
14	01F0 - 01F7	Intel 82371AB/EB PCI Bus Master IDE Controller
14	01F0 - 01F7	Primary IDE controller (dual fifo)
15	0170 – 0177	Intel 82371AB/EB PCI Bus Master IDE Controller
15	0170 - 0177	Secondary IDE controller (dual fifo)

Note that this computer has just one free interrupt request line, IRQ3. Note also that no IRQ is assigned to the computer's second serial port, COM2:. If a PCMCIA-based card is installed, that card may be assigned to IRQ3 by the Windows Plug-and-Play system.

3.13 Equipping a Desktop Computer with Multiple Modems

See http://www.sandstorm.net/support/phonesweep/multiport.shtml for up-to-date information on recommended multi-port solutions.

There are many strategies for configuring a desktop computer to use multiple modems:

- The simplest is to equip your computer with a PCI or USB-based multi-port serial I/O expander and use external modems.
- Sandstorm recommends SeaLevel's Versa-COMM 4-port (model 7401) and 8-port (model 7801) cards (http://www.sealevel.com/). (**Important Note:** You must install the Asynchronous driver from the SeaLevel CD **before** installing the SeaLevel card. Also, if you are using an old card, or upgrading to a new OS, please obtain the latest drivers from SeaLevel's website. You can install multiple SeaLevel cards on your system (*Windows NT does not support the use of multiple multi-port serial I/O cards*).
- 8 Modems: Digi (http://www.digi.com), has some very good solutions for 8+ port operation, including the AccelePort and Edgeport USB devices.
- 4 Modems only: You can use two of SIIG's Cyberserial PCI-Bus High-Speed Dual Serial Port cards (model # IO1888) (http://www.siig.com/products/io/pci_io.html).
- Avoid interface cards by Addonix; they have been found to have unreliable software drivers.
- You can also install an ISA-based multi-port serial I/O card and use external modems.
- The most difficult alternative is to **install one or more single or dual COM port cards or internal modems**. This requires assigning each COM port or modem to its own IRQ and I/O address.

We recommend using a USB or PCI multi-port serial expander if possible. This avoids any issues related to PC IRQs and I/O addresses. Otherwise, you may need to remove other hardware to free up sufficient IRQs and I/O addresses for that which you need to install. You may be able to remove or disable devices that are unnecessary in a production environment, such as sound cards and infrared ports. If you have unused devices built into your computer's motherboard, they can be disabled using the computer's BIOS SETUP utility.

3.13.1 Installation advice for multi-port cards

- When installing **SeaLevel cards** you must install the Asynchronous drivers **before** you install the physical cards. To install the drivers, you can either run *setup.exe* from the Start->Run dialog box, or open the *index.htm* file on the CD. (On the *index.htm* page, select the Install Software link, and then go to the Asynchronous section).
- **For all other multi-port cards** except SeaLevel, install the drivers after you install the hardware. Make sure you install the correct drivers for your operating system.
    - With the Power off, place each card into its slot dead-on (not at an angle) so that all electrical connections come together at the same time. This will synchronize communication with the PC.
    - Push the card gently into each slot. Some PC's make an audible click when the card is fully in place.
    - When plugging the multi-port card and modems into the octopus cable, be sure all connections are dead-on. Some connections are very fragile; be very careful how you push the cable onto the card.

- Once you have installed the multi-port card, octopus cable(s), and drivers, check your COM ports as follows:
- Open the Systems Properties box in the Control Panel, and select the Device Manager tab.
- Check Multi-port Devices. Your card should be listed there.
- Check COM ports under Ports (COM and LPT):
  - For 4 ports, COM ports 5-8 should have modem drivers.
  - For 8 ports, COM ports 5-12 should have modem drivers.
  - For 16 ports, sometimes the drivers for the large multi-port cards will install COM ports with higher numbers. The Perle SX+PCI card (see below), allows you to assign which COM ports the card uses. This is not a problem, as PhoneSweep can operate on any COM port up to 255.

If you only see modem drivers for ports 1-10 or 5-10 you will need to use the Add New Hardware program in the Control Panel to manually install modem drivers on ports 11 and 12. The **Dell Latitude Desktop PC** is known to have this problem. In the case of large multi-ports, you may need to go through the Add New Hardware program for all ports. It all depends on the desktop computer model.

3.14 Equipping a Desktop with multiple modems for PhoneSweep Plus 12 and 16

There are 4 basic strategies for equipping a desktop with 12 and 16 modems for use with PhoneSweep Plus 12 and 16.

- **Digi AccellePort 16em** (http://www.digi.com) multi-port card provides 16 serial I/O ports for your desktop, connecting through a PCI card. (Tested and approved on Windows 98 and 2000. We have not tested the Digi Accelleport with Windows 95 or Windows NT)
- **Perle** (http://www.perle.com) **SX+PCI** (1 card), **plus SXDC8/MX** (two 8-port units), which has been tested and approved by Sandstorm for Windows 2000 and NT 4.0 only. PhoneSweep has not approved this solution for Windows 95 and 98.
- **Digi Edgeport 416 Multiport USB** provides 16 serial I/O ports and 4 USB ports for your desktop or laptop, connecting through the USB port of your computer. Approved for Windows XP and 2000 only. We couldn't get this to work properly on Windows 98, thus Sandstorm does not approve the Edgeport for that platform. Windows 95 and NT have no USB capabilities. The 416 can be ordered with either 9-pin or 25-pin serial connections. Be sure to order the appropriate connectors for your configuration.
- You can use **multiple multi-port Serial-I/O cards in Windows 95, 98 and 2000**, as long as you have enough slots. We recommend in this case that you use Versa-Com 4-port (model 7401) and 8-port (model 7801) cards by SeaLevel. As always, please note that you must install the SeaLevel asynchronous card drivers before you install the card.
  - For PS Plus 12: one 8-port card (model 7801) and one 4-port card (model 7401).
  - For PS Plus 16: two 8-port cards (model 7801).

With any of these solutions, you can use a **Multi-Tech ZDX Modem Rack** (http://www.multitech.com), which takes up to 12 Multi-Tech modems. For PhoneSweep Plus 16, you would need 4 additional modems that would sit next to the modem rack.

3.15 Equipping a Laptop with Multiple Modems

Before selecting a laptop computer to run PhoneSweep Plus or Plus 8/12/16, be aware that PhoneSweep has historically had fewer problems on laptops running Windows 95, 98, or 2000 than on those running Windows NT. Windows NT, in fact, does not support the simultaneous use of two Quatech 4-port PCMCIA cards. For this reason, PhoneSweep Plus 8 is not supported for Windows NT on laptops.

There are several ways to equip a laptop computer with more than one modem (up to 8 modems):

- Install up to two multi-port PCMCIA serial cards. Sandstorm recommends the Quatech QSP-100 (http://www.quatech.com). Note that Quatech's Windows NT drivers only support two QSP-100 cards. For this reason, PhoneSweep Plus8 is not supported on Windows NT laptops.
- Add one or two PCMCIA modem cards or USB modems to the computer. Please see our list of Recommended Modems in **Section 3.8**.
- If the laptop has a serial port, connect an external modem to it.
- If you have a USB interface, Sandstorm has recommended USB multi-port solutions. See http://www.sandstorm.net/support/phonesweep/multiport.shtml for further details.

3.16 Uninstalling PhoneSweep

To uninstall PhoneSweep, click on the **Add/Remove Programs** icon under the Control Panel. Scroll down to the PhoneSweep entry, click on the **"Remove"** button, and confirm your choice.

Because the information in PhoneSweep profiles may represent weeks or months of work, **database files containing information from PhoneSweep scans are not removed by the uninstaller.** These database files are kept in the Profiles subdirectory in the main Sandstorm directory. If you wish to remove the PhoneSweep profiles, you can do so by manually dragging the main PhoneSweep directory to the Recycle Bin after uninstalling PhoneSweep.

3.17 Reinstalling PhoneSweep

PhoneSweep does not store its configuration in the Windows Registry. For this reason, the program is relatively resistant to bad interactions with other software or file corruption. Nevertheless, if you have problems with PhoneSweep that don't seem related to changes in your hardware configuration, or if the PhoneSweep program files become corrupted, you can safely reinstall PhoneSweep at any time. You do not need to specifically uninstall PhoneSweep before reinstalling it. Note that you cannot reinstall PhoneSweep while the previous installation is running.

If you have modified the *phonesweep.ini* file, save a copy in a different directory or under a different name before reinstalling PhoneSweep. Reinstalling PhoneSweep will overwrite any previous *phonesweep.ini.* After PhoneSweep is reinstalled, copy the old *phonesweep.ini* file over the new one.

You will not lose information in existing profiles when you reinstall PhoneSweep. No profiles are copied or created by the PhoneSweep installation process, so nothing will be overwritten. If you suspect that the installation files have been removed or corrupted, reinstall PhoneSweep.

4 Setting Up a Sweep

Before you can start a PhoneSweep scan, you must give the details of what is to be scanned and the parameters to use during that scan. These steps will get PhoneSweep ready to scan:

- Click on the **Setup->Profile** sub-tab to either select an existing profile to scan or to create a new profile (you can have as many profiles as you have memory for). **Or,** click on the **Copy** icon to make a copy of the current open profile, or click on the **Rescan** icon to make a to make a copy of the current open profile and open to it.
- Click on the **Phone Numbers** tab to either enter a new list of phone numbers to call and the time periods in which to call them and any associated notes, or to modify the numbers in an existing profile. Or, you can click on the **Import** button at the top of the user interface to import phone numbers from a *.txt* or *.csv* file.
- Click on the **Setup->Modem** sub-tab to select and configure the modems you will use to perform the scan.
- Click on the **Setup->Time** sub-tab to adjust the time periods in which PhoneSweep will place calls, and how long it will wait for a response on each call.
- Click on the **Setup->Effort** sub-tab to specify what actions PhoneSweep will take when a call is answered by a modem.
- Click on the **Setup->Dialing** sub-tab to specify how PhoneSweep will dial remote telephone lines.
- Click on the **Start** button to begin your sweep!

4.1 Setting Up And Managing Calling Profiles

"**Profiles"** store all information associated with a set of phone numbers, including scanning preferences that apply to that set of numbers and the results of any calls made to those phone numbers during a sweep. PhoneSweep displays the name of the current open profile along the very top of the PhoneSweep user interface.

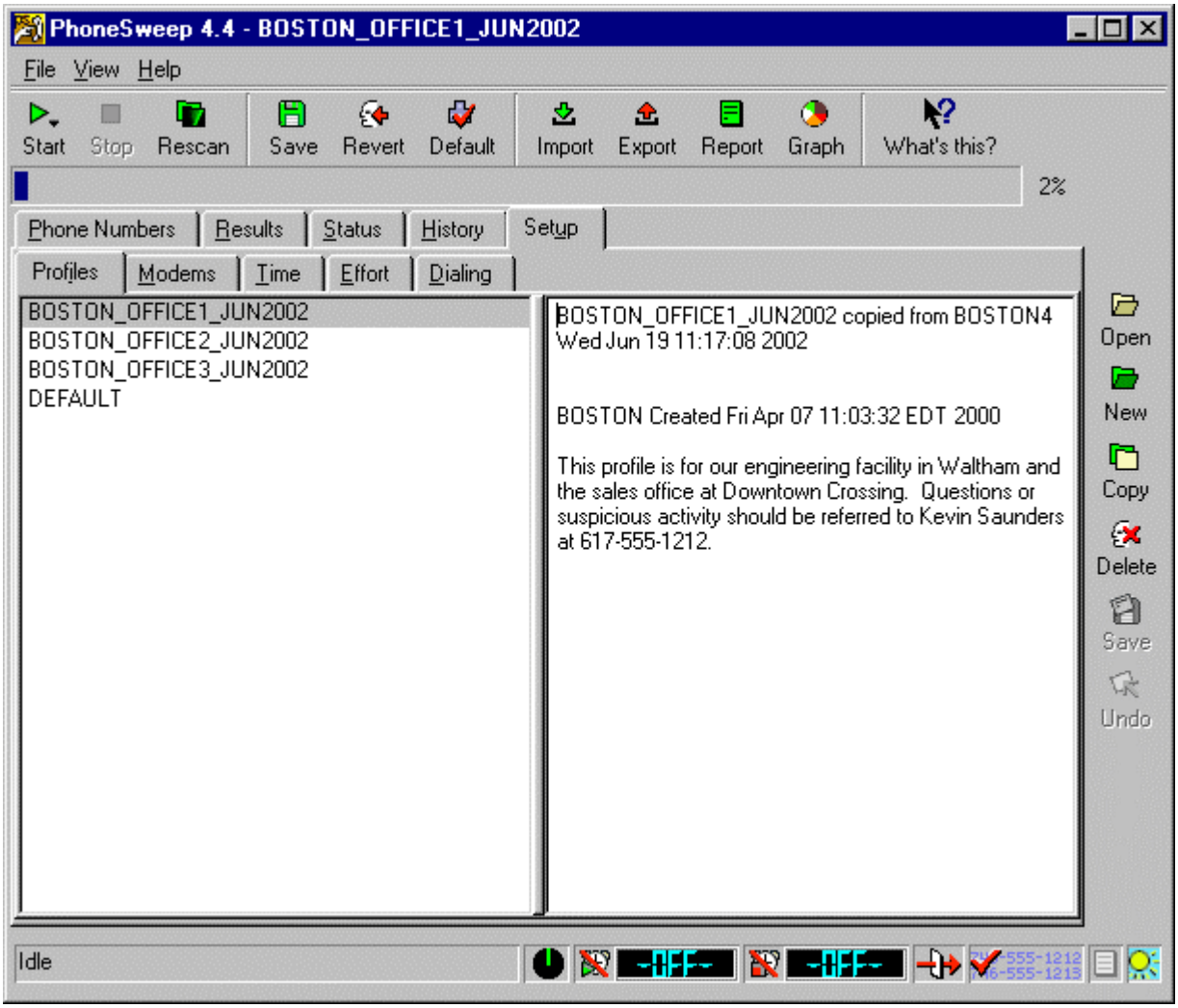
Each profile is its own database with call results stored as a set of records that PhoneSweep uses to generate reports. ***You only sweep a profile once***, so as not to skew the stored call results tabulation, and so that you can compare the results of two profiles to produce a *Differential Report*.

To rescan a set of phone numbers you can either click the **Rescan** button on the top of the PhoneSweep user interface, or click the **Copy** button on the **Setup->Profile** sub-tab. **Rescan** will copy the currently open profile, and automatically open the new profile. **Copy** copies the profile you have selected in the left pane of the **Setup->Profile** sub-tab, but does not automatically open it.

Sandstorm recommends that you ***never delete scanned numbers then add to numbers to scan, as this will skew the Call Results and Status tabulations for that profile. Doing this repeatedly to a profile can also corrupt the Call History Table for that profile.***

Information from each profile can also be drawn directly from the MySQL database for processing in other applications, such as Microsoft's Access program. (**Note: you must install the appropriate ODBC drivers in order to do this).**

To work with a profile, click on the **Setup** tab and then on the **Profile** sub-tab.



The **Profile** sub-tab view, found under the **Setup** tab, is divided into two parts:

- The left pane displays the Profiles List, which is a complete list of profiles currently in use by PhoneSweep. (At startup, PhoneSweep searches the **Profiles folder** for any database file beginning with "PS_". If you have a removed a "PS_name" folder from the **Profiles folder**, that profile will not be displayed on the Profiles List.).
- The right pane displays the Profile Note for the highlighted profile in the Profiles List.

4.1.1 What information is contained in a profile?

Each calling profile contains:

- A list of phone numbers and associated time period and note information.
- Information about calls already made to those phone numbers.
- Whatever scanning preferences have been set.
- A note that contains any comments you want to associate with the profile.

PhoneSweep's SQL database allows you to maintain a large number of phone numbers within each profile. Up to 800 phone numbers may be kept in each PhoneSweep Basic profile, and as many as 10,000

phone numbers can be kept in each PhoneSweep Plus or Plus8 profile and 20,000 numbers can be kept in each PhoneSweep Plus 12 and Plus 16 profile.

Note that these limits are *per profile*, not per-program. ***There is no limit on the number of profiles you can set up***, although you may find that profiles become difficult to manage once you have over 100 or so. In this case, you can copy the profiles you don't need immediate access to into another directory, or use a backup utility to archive them. *(Profiles are stored in the PhoneSweep Directory in the Profiles Subdirectory. You would save any folder beginning with "**PS_**".)*

Please note that Excel Spreadsheets may not be able to contain information exported from large profiles. The ***Excel spreadsheets have a limit on the number of entries each table can have.*** This will affect your ability to generate Charts, export results, and make some reports.

4.1.2 Overview of profile management

Note: Profile names can consist of up to 29 alphanumeric characters, as well "_". (PhoneSweep will in fact replace any spaces in each Profile's name with underscores "_").

- **Create a new profile:** Click on the **New** button. A **New Name** pop-up window will appear. Select the text area and type the name of the new profile.
- **Open an existing profile:** Select (highlight) the profile you want to open from the Profiles list and click the **Open** button. When you select a profile, its corresponding note is displayed in the right hand pane.
- **Copy a profile without opening to the new profile:** Select (Highlight) the Profile you want to copy from the Profiles list, then click the **Copy** button. A **New Name** pop-up window will appear. Select the text area and type the name of the new profile. After you have created the copy, in order to use it, you must explicitly **Open** it.
- **Copy the current active profile** (as seen on the top of the PhoneSweep Screen) **and then open to the new Profile**: click the **Rescan** button. A **New Name** pop-up window will appear. Select the text area and type the name of the new profile. You must click on **Start** to begin scanning the new profile.
- **Change the text of a note**: Click on the right hand pane of the **Profiles** sub-tab. This is the Note field. You can edit the existing note, remove text, or add new text. If you decide you do not want the changes you have made, click **Undo** to revert to the last saved note. If you do want the changes to take effect, click the **Save Note** button on the right hand side of the Profiles sub-tab. You must save or undo any changes to the text of a note before changing to a different profile. A profile's note field can contain up to 64K of text.

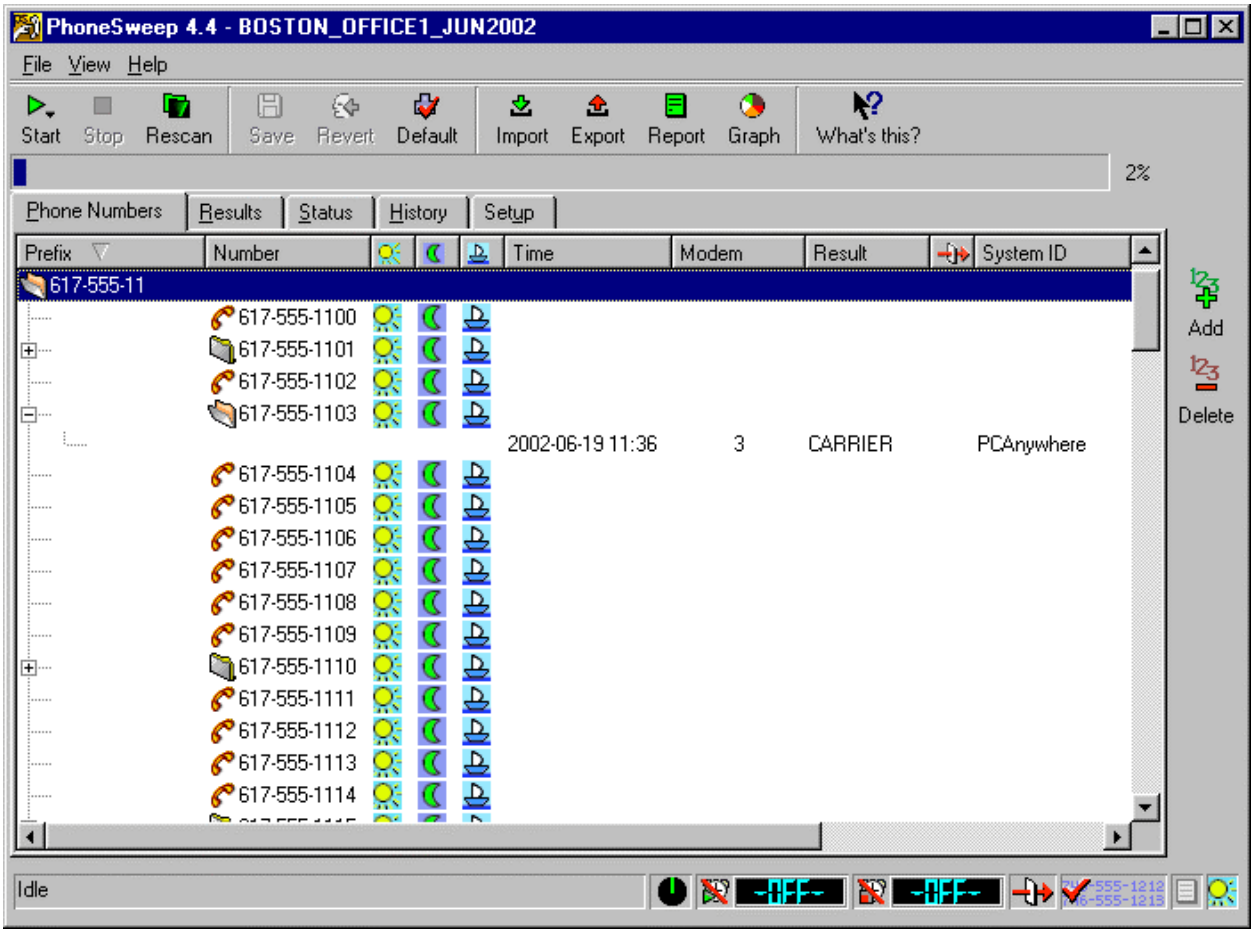
4.2 Adding Phone Numbers to a Profile

The **Phone Numbers** tab allows you to:

- **View and edit** the list of phone numbers in the current profile.
- **Specify and edit** the time period or periods (Business Hours, Outside Hours or Weekends) during which each number should be called.
- **View all calls that have been made to an individual number,** with call results.
- **Add and change notes** associated with individual or multiple phone numbers.
- **Set start and stop times** for the current profile.

Clicking on a folder allows you to see all the numbers in that particular folder, as well as the time period(s) in which each number is to be dialed.

Right-clicking on a folder brings up a pop-up menu that allows you to **expand or collapse** the current folder or all folders in the current view, as well as **"Find..."** text within the Phone Numbers tab. Searching will begin at the current folder.



4.2.1 What numbers can PhoneSweep call?

Before entering a phone number into a PhoneSweep profile, make sure that the number is can be dialed. Characters that PhoneSweep can dial include:

- any Touch Tone digit (0 through 9)
- space
- right and left parentheses
- period (.)
- comma (,)
- dash (-)
- hash mark or pound sign (#)
- asterisk or star (*)

- the letters x or X (for extension).

In other words, a legal phone number is a phone number made up of any characters in this list: **1 2 3 4 5 6 7 8 9 0 ( ) . , - * # x X**

Additionally, the special Touch Tones **A**, **B**, **C**, and **D** can be included in a phone number. Please note that these Touch Tones are not used in most telephone systems. If your phones have buttons labeled A, B, C and D, you should consult the phone switch documentation before telling PhoneSweep to dial these characters.

Characters in a telephone number that are not Touch Tones are called "formatting characters." They are allowed so that phone numbers are easier to read. The formatting characters are:

- Space
- Open and close parentheses
- Period
- Dash
- Capital or lowercase x

The **comma character** is not a Touch Tone, but **in the Hayes modem command set** it **causes the modem to pause between Touch Tone digits**, usually for two seconds.

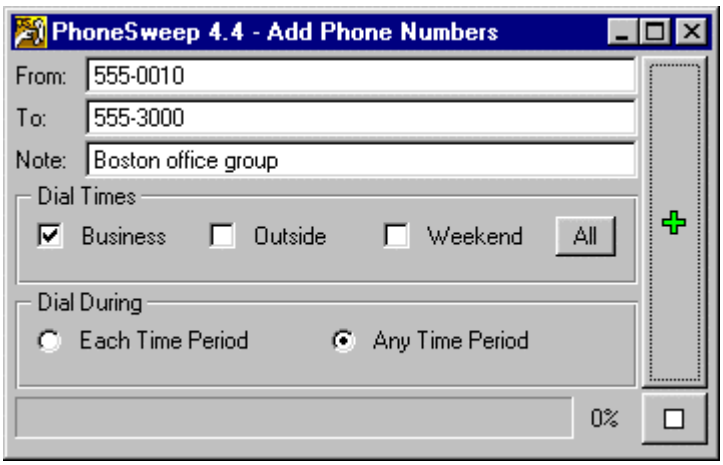
Phone numbers are limited to 31 characters in length. If you need to send more than 31 digits to place a call (for instance, if you're using a calling card or special access code, or if some dialing information may change based on your location), you can use the **Dial Prefix** and **Dial Suffix** options under the options **Setup->Dialing** sub-tab.

Also: Most modems can only dial a maximum of 50 characters which includes the prefix, phone number, and suffix Check your modem manual or with your modem's manufacturer for further details.

4.2.2 The Add Phone Numbers dialog box

To add Phone Numbers to a profile, click the **Add Phone Number** ( ) button on the right hand side of the **Phone Numbers** tab to bring up the **Add Phone Numbers** dialog box. . If you want to add phone numbers to an already existing Profile, be sure that it is the current Profile before clicking on Add Phone Numbers.

Note, that you can have phone numbers from any country and situation. For instance, you can place a main phone number for an automated system in the **Prefix** field on the **Setup-Dialing** sub-tab, then add the range of extensions via the **Add Phone Numbers** pop-up window. (You can then use commas in the **Prefix** field to make PhoneSweep pause between dialing the main number and then dialing the extension)



Use the **Add Phone Numbers** dialog box to:

- **Add either a single phone number or range of phone numbers** to the current open Profile.
- **Set time periods** for PhoneSweep to call each phone number or range of phone numbers
- **Set custom note** associated with each phone number or range of phone numbers
- **Set whether PhoneSweep should call each phone number during each time period** you specify, or **just make one call, which can occur during any of the time periods** that you specify.

Please note: When you have finished adding Phone numbers and related information below, Click **Add**. **Before clicking Add** you can click **Clear** to start over, or select a field and correct a mistake. Click the close button (X) when you are finished adding phone numbers to the profile.

4.2.3 Adding a single phone number or a range of phone numbers

To add a single number to the current profile: Type the number in the **From** field. Include any formatting characters needed to make the number readable. Consistent use of formatting characters in a profile will make the results of the sweep far more readable.

To add a range of phone numbers to the current profile: Type the starting number of the range in the **From** field, including any formatting characters. Then select or tab to the **To** field and type the last number in the range. The ending field will automatically include any formatting characters present in the starting number. PhoneSweep does not allow you to explicitly enter formatting characters in the ending number field.

When adding a range of numbers, the starting number must be the same length as the ending number. PhoneSweep assumes that you will start from the beginning of a range, such as 555-1000, and progress to a range endpoint of the same length, such as 555-2000. PhoneSweep will not add the range starting at 900 and ending at 1000 in a single command, but it will add the range starting at 0900 and ending at 1000. PhoneSweep will not add more than 10,000 numbers in a single range. In other words, adding 555-0000 to 555-9999 will work, but 555-1000 to **556**-2000 is not allowed.

If all phone numbers in the range start with the same character(s), you can place these character(s) in the prefix field located on the options **Setup->Dialing** sub-tab (see Section 4.7.1, **Setting dialing prefix and suffix**), rather than typing them in the Add Phone Number dialog box. This includes character(s) needed to dial an outside line (typically “9”).

4.2.4 Telling PhoneSweep when to call phone numbers (Time Periods)

The **Add a Phone Number** dialog box allows you to specify the time periods for PhoneSweep to dial a given phone number or range of phone numbers. Please note, PhoneSweep will not dial any phone number outside the hours you set for that number or range, though the radar-like Sweep Icon is moving ( ).

PhoneSweep supports three time periods:

- Business Hours (default 9:00-16:59)
- Outside Hours (all weekday hours other than business hours)
- Weekends (default Saturday and Sunday)

You can view and modify the default settings for these three periods on the **Time** sub-tab under the **Setup** tab (see Section 4.4, **Setting Time Options**).

To select the time period(s) for a phone number or range, click the appropriate check boxes next to the periods during which you want each number called. You can also specify whether each phone number or range of phone numbers should be called only once, during **any** time period, or during **each** of the time periods you specify.

Dial During Any Time Period will result in the phone number or range of numbers being dialed only once during the course of a scan.

Dial During Each Time Period will result in the phone number or range being dialed during each time period checked on the Add a Phone Number dialog box.

4.2.5 Adding Notes for a single phone number or range of phone numbers

The **Add Phone Numbers** dialog allows you to set a note for each phone number or range of phone numbers. Select the **Note** field and enter your note there, at the time you add the phone numbers.

4.2.6 Editing and deleting phone numbers and associated time periods and notes

There is no way in PhoneSweep to directly edit a phone number; however, you can change the time period and note associated with each phone number. To delete, go to the **Phone Numbers** tab and:

- For a **single phone number**: select the number you want to delete and click the **Delete** button at the right-hand side of the tab.
- For **multiple phone numbers**: highlight the phone numbers you want to delete. Then click the **Delete** button.
- For an **entire prefix**: select the folder with the prefix you want to delete, and click the **Delete** button. When doing this, be careful not to delete more numbers than you mean to!

To edit the time period or note for one or more numbers:

- For a **single phone number**: Right click on the phone number record, and choose **Alter Phone Number**.
- For **multiple phone numbers** in a prefix: Right click on the prefix folder, and choose **Alter Prefix**.

- For **all phone numbers in a Profile**: Right click on any prefix folder or phone number record, and choose **Alter All Phone Numbers**. This will alter the numbers you did *not* right-click, as well as the ones you did.

4.3 Setting Scheduled Start and Stop times

4.3.1 Schedule Sweep Start Time

Left-click and hold down the **Start** button to display the scheduling options popup, or bring up the submenu under **File->Start**. Click on **Schedule Start…**, then change the **Choose Hours/Minutes** fields to the desired start time, and click **Schedule**.

4.3.2 Schedule Sweep Stop Time

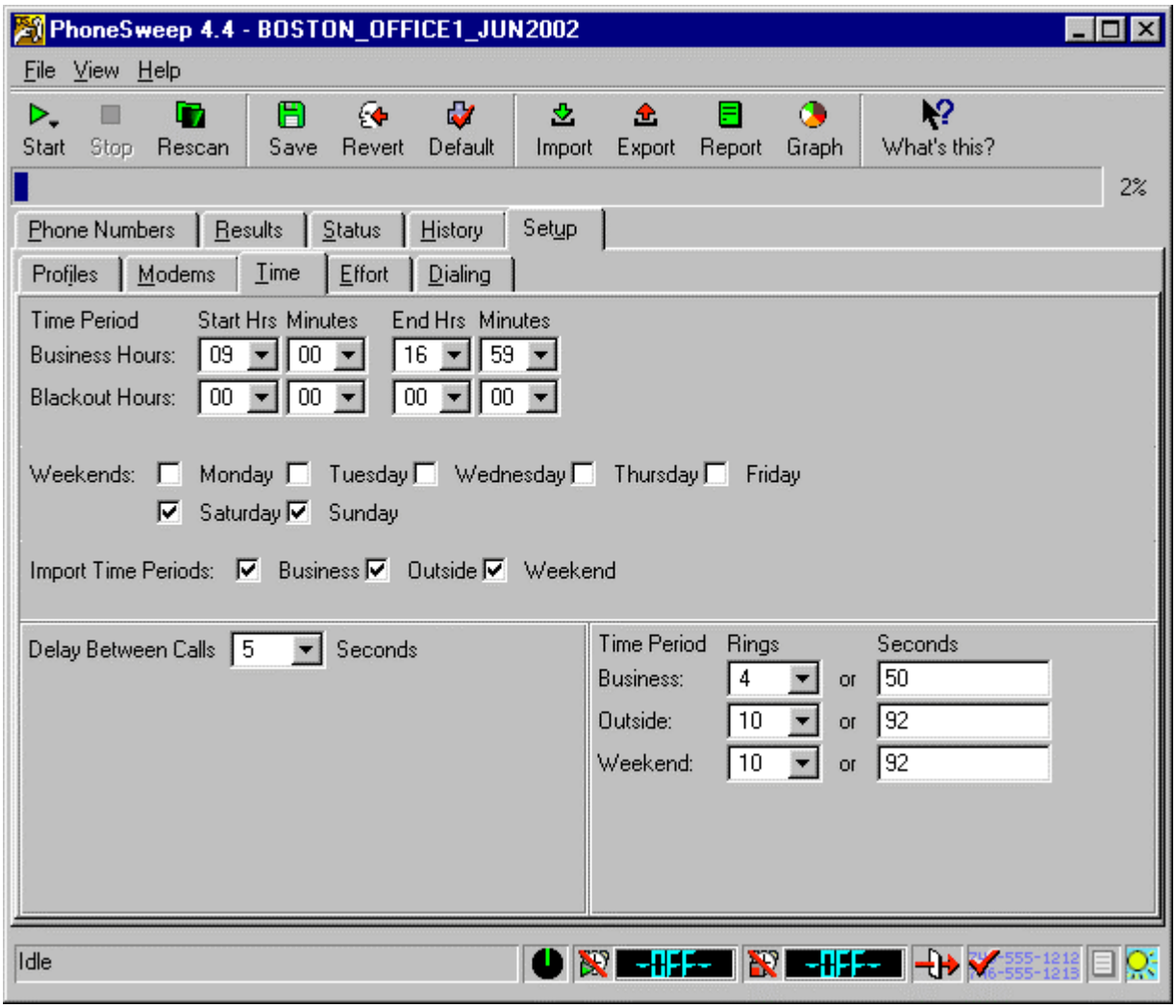
When a sweep is not running: Left-click and hold down the **Start** button to display the scheduling options popup, or bring up the submenu under **File->Start**. Click on **Schedule Stop…** then change the **Choose Hours/Minutes** fields to the desired stop time, and click **Schedule**.

When a sweep is running: Left-click and hold down the **Stop** button to display the scheduling options popup, or bring up the submenu under **File->Stop**. Click on **Schedule Stop…** then change the **Choose Hours/Minutes** fields to the desired stop time, and click **Schedule**.

4.3.3 Canceling Scheduled Starts and Stops

Left-click and hold down the **Start** button to display the scheduling options popup, or bring up the submenu under **File->Start**. Click on **Cancel Scheduled Start** or **Cancel Scheduled Stop**. Scheduled starts and stops are canceled automatically when you change profiles, but the start and stop times are remembered.

4.4 Setting Time Options


PhoneSweep 4.4 - BOSTON_OFFICE1_JUN2002
File View Help
Start Stop Rescan Save Revert Default Import Export Report Graph What's this?
2%
Phone Numbers Results Status History Setup
Profiles Modems Time Effort Dialing
Time Period Start Hrs Minutes End Hrs Minutes
Business Hours: 09 00 16 59
Blackout Hours: 00 00 00 00
Weekends: Monday Tuesday Wednesday Thursday Friday
Saturday Sunday
Import Time Periods: Business Outside Weekend
Delay Between Calls 5 Seconds
Time Period Rings Seconds
Business: 4 or 50
Outside: 10 or 92
Weekend: 10 or 92
Idle

The **Time** sub-tab, found under the options **Setup** tab, allows you to control time periods and other time related features that PhoneSweep uses when dialing:

- Define the time period designated **Business Hours** ( ) and by extension **Outside Business Hours** ( ).
- Define what days are weekends (subject to **Weekend** ( ) time period with 24 hour scanning), and by extension, weekdays (subject to Business Hours ( )and Outside Business Hours ( ) time periods)
- Set **Blackout Hours,** during which PhoneSweep will not call numbers assigned to be dialed during that time period.
- Set the **Delay Between Calls** (in seconds).
- Set how long PhoneSweep will wait for a response from a number it has called during a given time period (timeout in seconds).

- Set the *default* **Import Time Period(s)** which PhoneSweep assigns to phone numbers imported into a PhoneSweep profile without an accompanying time period code (See ***Importing and Exporting data***).

Note: The **Time** sub-tab **does not assign** time periods to phone numbers, except when you **Import** phone numbers without associated time period codes. **You can assign time periods** when you add or edit phone numbers on the **Phone Numbers** tab, which was covered in the previous section**.**

4.4.1 24-hour format

PhoneSweep works with times in 24-hour format. To get the 24-hour designation for any time after 12 noon, add 12 to the time you would usually use. For example, one o'clock in the morning would be represented in 24-hour format as "01:00" and one o'clock in the afternoon is represented as "13:00."

To select a time for Business Hours or Blackout Hours, click on the hours or minutes field, and choose the desired time from the pull-down menu.

4.4.2 Redefining time periods

By default, Business Hours start at "09:00" (9:00 AM) and end at "16:59" (4:59 PM). You can freely change the Business Hours, provided that the *start time always has a lower value than the stop time*.

Note: Since 00:00 is the beginning of the day and 23:59 is the end of the day, this means that the **period specified by Business Hours cannot cross midnight**.

If business hours at your site cross midnight, simply use outside hours to specify your business hours, then go to the **Phone Numbers** tab to assign numbers to dial during "Business Hours." Or, you can use Blackout Hours to control when PhoneSweep should not call numbers to dial during outside hours (See **Blackout Periods** below).

To modify the Business Hours field, click on the hours or minutes field as appropriate and choose the time from the pull-down menu.

4.4.3 Redefining weekdays and weekends

Selecting a day (checking it) will toggle it to being a weekend day, subject to the **Weekend** ( ) time period with 24 hour (00:00 to 23:59) dialing.

Unselecting (uncheck) a day, it becomes a Weekday, subject to Business Hours ( ) and Outside Business Hours ( ) time periods.

This allows you treat even Saturdays and Sundays as weekdays so you can scan during outside (evening) hours,

Or, you can treat other days (such as holidays) as weekends so that you can scan the full day while everyone is out of the office.

4.4.4 Blackout periods

Use **Blackout Start** and **Blackout Stop** to exclude a specific span of time from being dialed without changing the values of the time periods Business Hours, Outside Hours and Weekends.

Set **Blackout Start** to the beginning of the time span to be excluded from dialing, and set **Blackout End** to the end of the time span to be excluded. As before, time is specified in a 24-hour format. ***Note:*** *the value of Blackout Start must be smaller than or equal to the value of Blackout Stop.*

To set the Blackout Hours field, click on the hours or minutes field as appropriate and choose the desired time from the pull-down menu.

To remove a blackout you have specified, change Blackout Start and Blackout Stop to the same value or set both back to 00:00.

Note: You can set Blackout times to cover part of Business Hours; however, if you want to blackout business hours entirely, we recommend you do not use Blackout. Rather, you must assign phone numbers to dial only during Outside Business Hours, and if need be, to dial during weekends as well.

4.4.5 Setting time periods for imported phone numbers

The **Import Default Time Periods** section of the **Time** sub-tab specifies when numbers imported into PhoneSweep without individual time period values will be called. If you select the **All** button, the numbers will be dialed during any time period. Dialing during each time period requires multiple imports. (See **Importing and Exporting Data** for further information).

If you incorrectly assign the wrong **Import Time Periods** to use when you import phone numbers, you can **edit Time Periods on the Phone Numbers** tab.

4.4.6 Setting how long PhoneSweep will wait for a remote response

Set the length of time PhoneSweep will wait to receive a response from the number it has called by setting either the value of **Timeout in Rings** or **Timeout in Seconds** for each time period. With most modems, you must use the **Timeout in Seconds - this includes *ALL* Single Call Detect capable modems approved to date.** Therefore:

- When you change the **Timeout in Rings**, the **Timeout in Seconds** will automatically change to an appropriate value.
- However, you can change the **Timeout in Seconds** without changing the number of rings specified.

This means that when you have modems that support Remote Ringing, PhoneSweep will disconnect when the maximum number of rings have elapsed without receiving a response, and when you have modems that do not support Remote Ringing (most modems) PhoneSweep will disconnect when maximum number of seconds have elapsed without receiving a carrier tone.

Note that PhoneSweep's default timeout values for Business Hours are shorter than those values for Outside Business Hours and Weekends. Presumably, no one will be around at those latter time periods, so you can give PhoneSweep more time to pick up. Also, many business phone systems are set to use longer call pick up times during non-business hours.

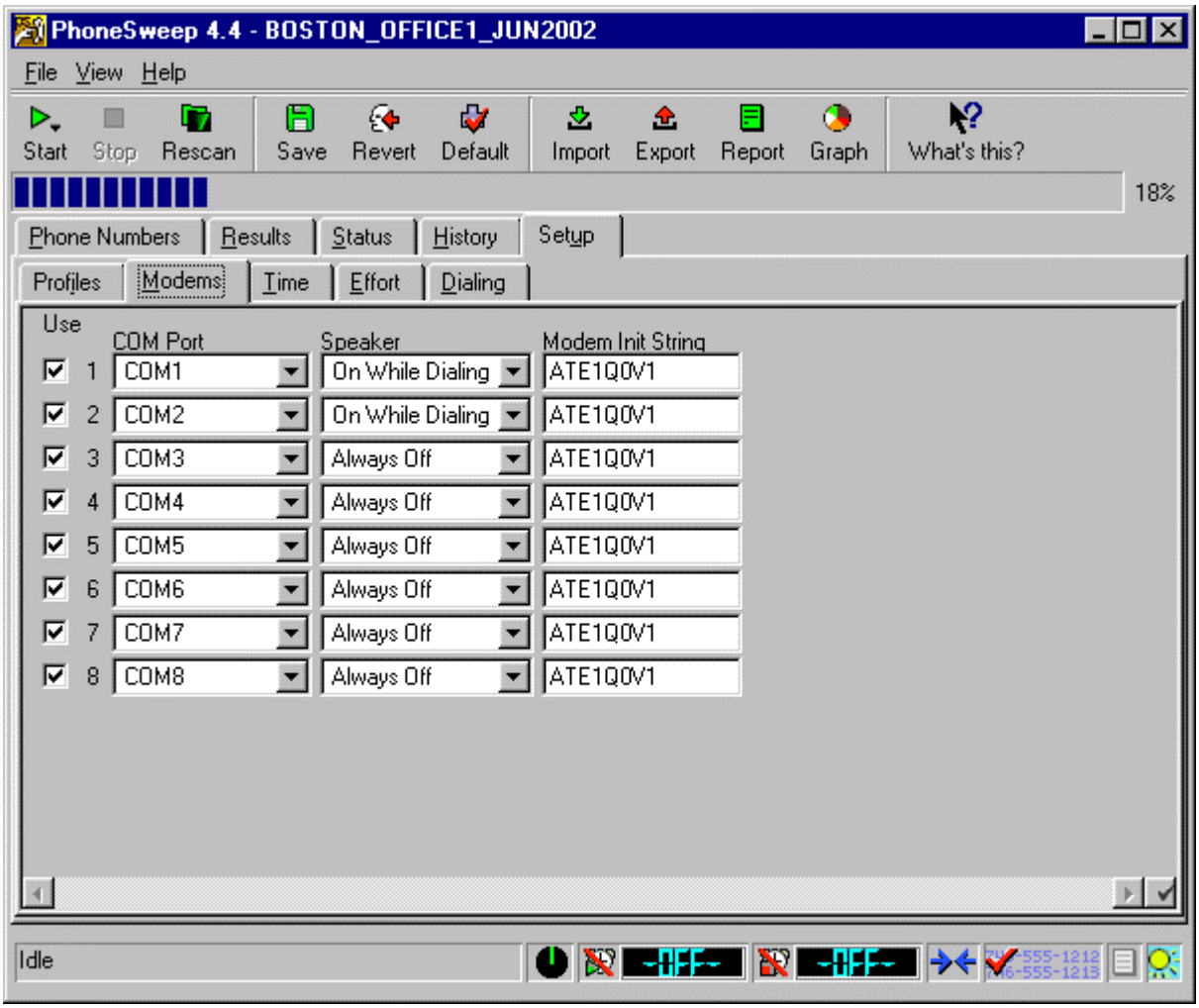
Note that the **Timeout in Seconds** value is an estimate for the correct number of rings, and may not be correct for your call setup time. We recommend that if the precise number of rings is important at a site, you should test PhoneSweep and carefully determine the correct number of seconds. **After Call Pick up:**

If you are using Single Call Detect, PhoneSweep will use the **Single Call Voice Timeout** (**Setup->Dialing** sub-tab) to determine how long to wait for a response after the line has been picked up.

If you are not using Single Call Detect, PhoneSweep will *only use* Timeout in Rings or Timeout in Seconds to determine how long to wait for a response. (Note that by default U.S. modems will wait 60 seconds, EU modems 50 seconds).

In Identify or Penetrate mode, after PhoneSweep receives a carrier (modem) signal: PhoneSweep will try for a period equal to the length of *Timeout in seconds* to get a username prompt. Each time PhoneSweep is able to send a username guess, it will reset its counter and wait Timeout in Seconds again.

4.5 Setting up your Modems


PhoneSweep 4.4 - BOSTON_OFFICE1_JUN2002
File View Help
Start Stop Rescan Save Revert Default Import Export Report Graph What's this?
18%
Phone Numbers Results Status History Setup
Profiles Modems Time Effort Dialing
Use COM Port Speaker Modem Init String
1 COM1 On While Dialing ATE1Q0V1
2 COM2 On While Dialing ATE1Q0V1
3 COM3 Always Off ATE1Q0V1
4 COM4 Always Off ATE1Q0V1
5 COM5 Always Off ATE1Q0V1
6 COM6 Always Off ATE1Q0V1
7 COM7 Always Off ATE1Q0V1
8 COM8 Always Off ATE1Q0V1
Idle
-OFF-
-OFF-

The **Modems** sub-tab, located under the **Setup** tab, displays modem configuration information for only the number of modems allowed by your PhoneSweep model license. Thus, you will see a line for one modem for PhoneSweep Basic, four for PhoneSweep Plus, eight for PhoneSweep Plus8, and so on.

For changes to take affect on this sub-tab, you need to select the **Save** icon along the top of the PhoneSweep UI.

The **Modems** sub-tab allows you to:

- Set which modems are to be used by this particular sweep (Select 1, only a few or all; you can select all modems at once by clicking on the **Select All Modems** button on the lower right corner of the **Modems** sub-tab (black check mark).
- Set which COM (serial) port each modem is connected to.
- Set initialization strings for each modem.
- Control the modems' speakers individually.

You can set options for all modems at once by using the **right-click menu**. This provides one-click setting of use status, speaker setting and init string for all modems to the same value as the item right-

clicked upon. You can also renumber the COM ports for all modems starting at the item right-clicked upon. These settings will not be saved until you click the **Save** button.

In order to sweep, PhoneSweep requires at least one modem to be powered on and connected to the computer, and the correct COM port must be assigned for each modem on the **Modems** sub-tab before PhoneSweep can detect the modem.

4.5.1 Windows and your modem

PhoneSweep bypasses the Windows TAPI (Telephone API) and communicates directly with the modems**.** For this reason, PhoneSweep does not require that you install the Windows modem drivers supplied by the vendor. Doing so won't interfere with PhoneSweep and may be required to use the modems with other applications when not sweeping. For this reason, **the Modems sub-tab does not automatically detect modems until you configure the Modem-to-COM port mapping using the Modems sub-tab.** (See below for further instructions.)

To determine which COM ports your modems are connected to, run *checkmodems.exe.* When using multi-port cards, such as SeaLevel cards on PCs and Quatech cards on laptops, you will find the COM ports run from COM 5 to COM 8 for 4 ports, and from COM 5 to COM12 for 8 ports.

4.5.2 Configuring the Modems sub-tab

To change the value of any white field on the **Modems** sub-tab, click on the down arrow to the right each field and a pull-down menu will appear.

First, enable the modems to be used in the sweep. Click in the **Use** box located to the left of each modem, or Click the **Select All Modems** button on the lower right hand corner of the **Modems** sub-tab. The Use box will display a check mark when a particular modem is enabled. As noted above, the **Modems** sub-tab displays only the number of modems licensed for your use. If you see a discrepancy in the number of licensed modems you expect to see, please contact Sandstorm Enterprises.

Then set the COM Port column to the correct value. If you do not know which COM ports your modems are connected to, you can use the *checkmodems.exe*. Once you know which COM ports your modems are connected to, set the COM: Port column to the correct value by single clicking on a Port column entry and choosing the correct value from the pull-down menu. The COM port will default to the same value as the modem number, but this is not required. Each modem must be on a different COM port. If two modems are set to the same COM port, PhoneSweep will not begin sweeping, even if one of them is not currently selected.

Specify whether Modem Speakers are turned on or off. Click on the pull down menu under the speaker heading for each modem to choose among three speaker options:

- **Always Off**: This modem will dial silently.
- **On During Dialing**: You will hear the modem dialing and any response from the remote system until a carrier has been established. After the connection has been established, the modem speaker will be disabled for the remainder of the call.
- **Always On**: Your modem speaker(s) will be on throughout the scan. We do not recommend this mode for normal use, as the noise can be quite irritating, but it can be useful in checking problem phone numbers. (Default setting)

Specify Modem Initialization Strings. Initialization strings are commands that are sent directly to the modem to specify various aspects of its behavior. Type any modem initialization strings directly in the box to the right of the appropriate speaker control for each modem. Remember to leave the letters AT at the start of your initialization string. (PhoneSweep's default initialization string for each modem is: ATE1Q0V1).

Important: Do not use the command **&W** in your initialization strings. This will write to the flash ROM of the modem. Since PhoneSweep sends the initialization string before every call, this will burn out the flash ROM after a few thousand calls.

Initialization strings are not well standardized. Therefore, we recommend that you check the documentation for your particular modem for more specific information. The following table contains some of the more common initialization settings.

Initialization String	Description
ATS6=x	"x" denotes the number of seconds your modem will wait for a dial tone. Increasing this can be helpful where PhoneSweep disables a modem because it does not get dial tone in time.
ATS7=x	"x" denotes the number of seconds your modem will wait for carrier. The common (U.S.) default is 60 seconds, though European modems are set to 50 seconds. This must be at least as large as the Timeout in Seconds value set on the **Time** sub-tab.
ATS8=x	"x" denotes the number of seconds that the comma character causes the modem to pause. The common default is 2 seconds. Increase this value only if you want to reduce the number of comma characters required to specify a pause interval.
ATS11=x	"x" is the length in milliseconds of each Touch Tone. If you are scanning an older phone system, you may need to increase the value to ensure that your phone system will recognize each digit dialed.

If you need to use multiple commands, they should be in the format **ATS6=xS7=x**.

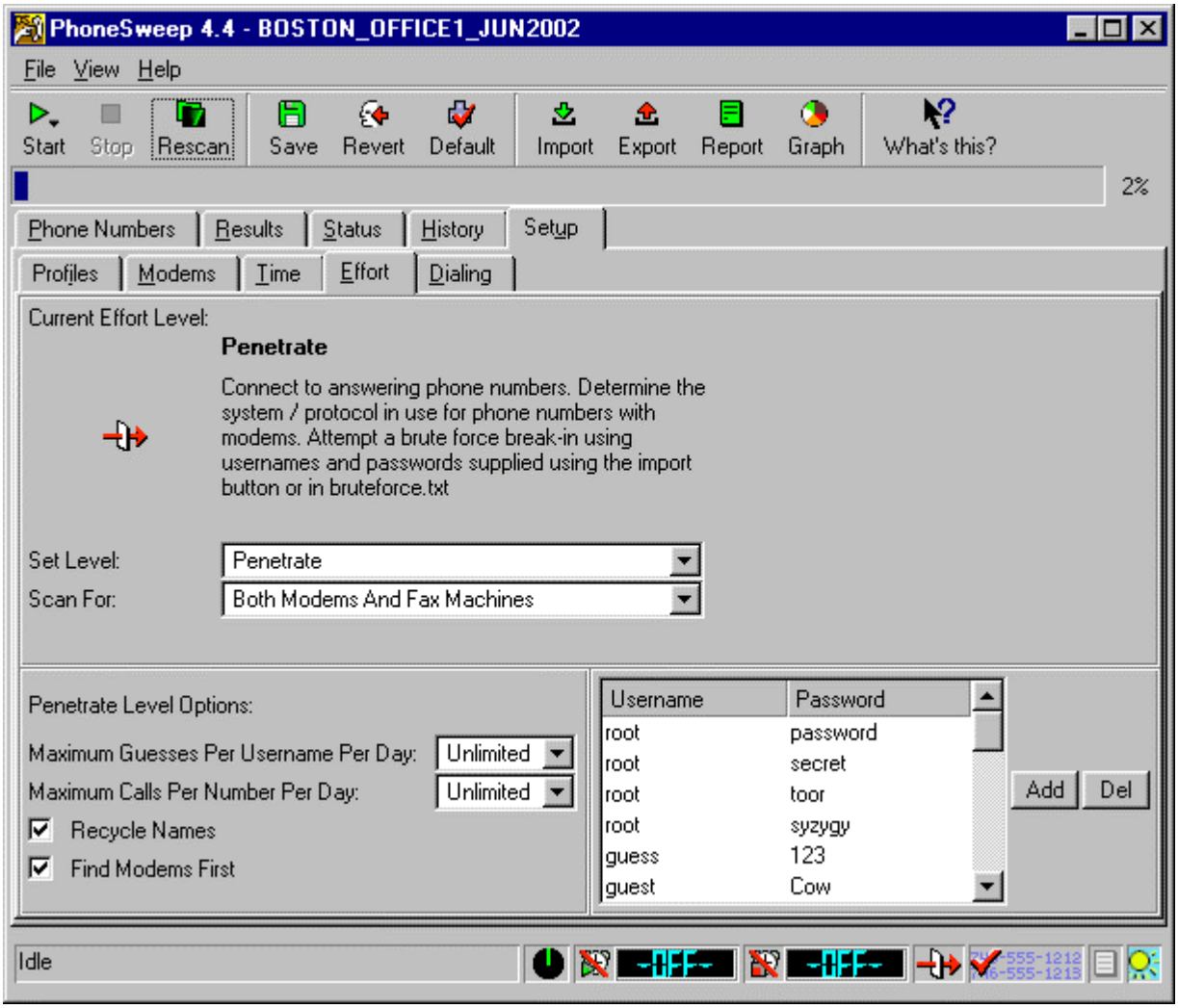
After you have set up your modems, click the **Save** button.

PhoneSweep will prompt you if you try to quit the program or start a sweep without saving your changes. These settings can be changed at any time during a sweep, but they will not take effect until the next call the modem makes.

The modem baud rate is set on the **Dialing** sub-tab, under the options **Setup** tab.

4.6 Setting Level of Effort

The **Effort** sub-tab, located under the **Setup** tab, controls which **Level of Effort** PhoneSweep will use when dialing phone numbers, as well as what actions to take in that mode. PhoneSweep automatically saves changes made on this sub-tab so you do not need to save changes by clicking on the **Save** icon.


PhoneSweep 4.4 - BOSTON_OFFICE1_JUN2002
File View Help
Start Stop Rescan Save Revert Default Import Export Report Graph What's this?
2%
Phone Numbers Results Status History Setup
Profiles Modems Time Effort Dialing
Current Effort Level:
Penetrate
Connect to answering phone numbers. Determine the system / protocol in use for phone numbers with modems. Attempt a brute force break-in using usernames and passwords supplied using the import button or in bruteforce.txt
Set Level: Penetrate
Scan For: Both Modems And Fax Machines
Penetrate Level Options:
Maximum Guesses Per Username Per Day: Unlimited
Maximum Calls Per Number Per Day: Unlimited
Recycle Names
Find Modems First
Username Password
root password
root secret
root toor
root syzygy
guess 123
guest Cow
Add Del
Idle

The **Effort** sub-tab allows you to:

- **Set Level (of Effort)**, which controls how much information PhoneSweep will attempt to gather when it calls each phone number.

- **Connect** ( ): PhoneSweep merely attempts to determine what type of line it is calling (Voice, Fax, Carrier/Modem, etc.) by listening to the line then hanging up (No data exchanged).
- **Identify** ( ): PhoneSweep attempts to identify remote systems by exchanging an electronic handshake, then immediately hangs up.

- **Penetrate** ( ): PhoneSweep attempts bruteforce (guess) username/password combinations on systems it was able to Identify. If successful, PhoneSweep will immediately hang up and go no further.
    - Control what PhoneSweep will **scan for** (All Levels of Effort):
- **Both Modems and Fax Machines** where Phone Sweep will call twice to search for Fax/Modem lines (Voice and other lines called once).
- **Modems only** where PhoneSweep will call each line just once as it searches for just modems.
- **Fax Machines only** where PhoneSweep will call each line just once as it searches for just fax machines.
    - **Fine-Tune Penetrate Level of Effort (Penetrate** sub- options), telling PhoneSweep to:
- **Recycle** username/password combinations (Try to use every username/password at every modem it encounters).
- **Find Modems First**, where PhoneSweep will first sweep all phone lines in its search for modems before returning (going back) to brute-force the modems it found. Otherwise, PhoneSweep will attempt to brute-force each modem as it finds them.
- **Limit guesses or calls** in a given day, to avoid being locked out of systems.
- **View and edit** the username/password list**.**

See Section 10.1 "**Expected Sweep Result Charts**", for additional details on PhoneSweep results when scanning with and without Single Call Detect at various Levels of Effort, and when scanning for both fax and modems, modems only and fax machines only.

4.6.1 What does PhoneSweep do at each level of effort?

- **Connect**: **PhoneSweep identifies each device by sound or tone alone so that no exchange of data occurs:** As PhoneSweep makes each call it listens and classifies each line, according to the sounds it hears, including if an answering device and whether or not it is a Carrier or Fax, and then, PhoneSweep immediately hangs up.
- **Identify**: **If PhoneSweep finds a modem, it attempts to determine the type of system that modem is attached to.** *An actual exchange of information occurs at this level (electronic handshake).* This may involve sending some information to the remote device, most likely carriage returns.
- **Penetrate**: **PhoneSweep returns to each modem it has found and attempt to break into the remote system with a brute-force username/password guessing attack.** At this level, PhoneSweep not only performs the initial electronic handshake with each fax or modem, but also attempts to exchange logon information with any system it encounters, providing bruteforcing information is known by Sandstorm about that system.

Each successively more invasive **"level of effort,"** includes all less invasive levels by default. So, when you **identify** remote systems, PhoneSweep must first **connect** to them. If you set PhoneSweep to **Penetrate**, it will also **connect** and attempt to **identify** before attempting to break into the system.

Please note, that with regards to PhoneSweep and System Identification, *PhoneSweep should not affect systems*. In rare instances; however, some systems cause PhoneSweep to freeze. In even rarer instances, the box PhoneSweep is on will freeze.

If PhoneSweep does freeze during a sweep, please do not restart PhoneSweep. Instead save a copy of the *phonesweep.log* to send to Sandstorm Support, noting if there were any other programs, virus checkers or network connection attempts during the time of the sweep. Sandstorm support will then attempt to identify which number caused problems with PhoneSweep. The Penetrate level of effort can be dangerous!

Caution: When you set PhoneSweep to scan at the Penetrate level of effort, PhoneSweep will attempt to break in to any devices it finds on the other end of the line. Doing this without proper authority may be a violation of applicable laws. Be sure that you understand what Penetrate mode does, that you wish PhoneSweep to scan at the Penetrate level, and that you have clear authorization to perform a PhoneSweep scan at the Penetrate level.

4.6.2 Username/password recycling

Username/password recycling is only relevant at the **Penetrate level of effort**. PhoneSweep's default setting is to have **username/password recycling** on (checked).

If you know that all of the modems you are attempting to call are connected to the same system, or a set of systems that share a common username/password database (e.g. a single RADIUS server), you can keep PhoneSweep from making redundant calls by disabling username/password recycling.

Username/password combinations can be:

- **recycled**: each combination of username/password (listed in the Setup -> Effort tab)used on every remote modem found.
- **not recycled**: only used once during a sweep.

On many systems, PhoneSweep can try three username/password combinations per call; however, PPP authentication protocols only allow one attempt per call. If you choose to recycle the username/password combinations, PhoneSweep will need to make many more calls than it otherwise would, and thus will take *significantly* longer to complete the scan.

You should disable username/password recycling when leaving it enabled would cause PhoneSweep to make redundant penetration attempts, and therefore unnecessary calls. This is the case if you know that all the modems that you are trying to dial are connected to the same system, as in the case of a modem pool. If ten remote numbers connect to the same terminal server, which has only one username/password database, there is no reason to a try given username/password combination on more than one of the remote numbers.

4.6.3 Using multiple profiles to optimize large scans

You may want to use profiles to split your pool of phone numbers into smaller sets for more efficient scanning. For instance, say you wish to brute-force modems found on a previous scan. The numbers fall into three categories: ten connect to a time-sharing system, twenty more are the hunt group for a dial-up server, and the remaining fifteen are miscellaneous phone lines. In this case, you would create three profiles:

Content of Profile	Should recycling be enabled?
Ten phone lines on first system	**No** – these phone lines all reach the same system and a single username/password database.
Twenty phone lines on second system	**No** – these phone lines also share a single username/password database
Fifteen miscellaneous phone lines	**Yes** – Any modems connected to these phone lines probably reach multiple systems, each with its own username/password database.

Small profiles are also easier to recreate and rescan if data gets corrupted from such occurrences as the computer's plug getting pulled or during a blackout (this has happened to customers with large profiles).

4.6.4 Find Modems First

The **Find Modems First** check box controls the order of operations in a Penetrate-mode scan and comes checked as a default setting.

When checked, PhoneSweep first scans all numbers in a profile to identify which ones have modems, and then goes back and attempt to bruteforce the modems it has discovered.

Find Modems First should always be enabled if username/password recycling is active; otherwise PhoneSweep will try its entire username/password database against the first modem it discovers before proceeding to any other number.

4.6.5 Limiting numbers of calls and brute-force attempts

Some systems lock a user out if there are too many unsuccessful attempts to log in to their account. Therefore, PhoneSweep can be configured to set the maximum calls per phone number per day, as well as maximum guesses per username per day. PhoneSweep's default value for both is Unlimited. Use the scrollbar in the lower left corner of the Effort dialog box to change these values.

If you limit the number of guesses per username per day, you should also limit the calls per number per day. If you do not do this, PhoneSweep may call numbers that it cannot brute-force because that guess would exceed the number of guesses per username per day. This results in a situation where PhoneSweep cannot make any username/password guesses, but continues to dial phone numbers.

We do not recommend that maximum calls per day be limited when performing a scan in Sequential mode. Limiting the maximum number of calls per day during a sequential scan may result in PhoneSweep stopping, unable to make any calls. This happens when the next number in sequence has already been called the allowed number of times.

If PhoneSweep calls a number that turns out to be busy, that call does not count against the maximum number of calls that can be made to that number per day, since the call was not completed.

After you have configured PhoneSweep to the correct level of effort, be sure to save any changes you have made.

4.6.6 The *bruteforce.txt* file

In Penetrate level of effort, PhoneSweep uses a file called *bruteforce.txt*, as username/password combinations that PhoneSweep will use when it attempts to break into remote systems. This file is initially read into an internal database for each **new** profile created, and can be viewed via the Setup->Effort tab. When a profile is copied using **Copy** or **Rescan**, the internal database is copied as well. The

bruteforce.txt file initially installed with PhoneSweep contains a basic list of common username/password combinations, but most users will need to make changes to it to suit the needs of their organizations. Changes can be made in any of these ways:

1. Edit the username/password list directly on the **Effort** tab. These changes will be recorded to the internal database. If you want the changes to be applied to the *bruteforce.txt* file, use the **Export** button to export the changes to the file.
2. Use ***brutecreate.exe*** to add to the bruteforce.txt file (combining separate Username and Password files to add to the bruteforce.txt file), then create a new profile or import the file into PhoneSweep.
3. Edit *bruteforce.txt* directly using a text editor, then create a new profile or import the file into PhoneSweep.
4. Create your own source file directly with a text editor, and import it into PhoneSweep (see Section 6.2, **Importing Brute Force Information**).

(If you are editing or creating a file, use care if all you have available is a word processor - the file format *must* be MS-DOS style text with line breaks).

Three additional source files are included with PhoneSweep:

- ***largebrute.txt*:** This file contains the dictionary of passwords that hackers commonly use. This file can be used with *brutecreate.exe*.
- ***largebruteback.txt:*** This file contains the same dictionary words as *largebrute.txt*, but each of them is backwards. This file can be used with *brutecreate.exe*.
- ***systemdefault.txt:*** This resource file contains a master list of default usernames and passwords used by many common operating systems. *Use this file as a resource for sweeping against systems in your workplace in order to verify that default username/ password settings have been changed.* The file is organized by operating system; so you can *copy the appropriate usernames/passwords and paste them into your bruteforce.txt* file. This file *cannot* be used with *brutecreate.exe*.

Formatting for bruteforce.txt*:* Enclose the username and password by double-quote characters, and separate each username/password combination by a carriage return/line feed. Any text that is not enclosed in a double quote will be ignored. You can have blank User Names and Passwords (two double quotes, no spaces: “”). **Note:** Whether you use *bruteforce.txt* or create your own source file to import, you must use this format.

For example,

`"root","password"`	Example PhoneSweep 'bruteforce.txt' file
`“” ,“guest”`	This shows a blank UserName and a Password
`“admin”,“”`	This shows a UserName of admin and a blank Password

If username/password guessing restrictions are in effect*,* the bruteforce.txt file should be arranged so that the distinct usernames are distributed evenly through the password file, rather than arranged in blocks. This will help keep PhoneSweep from getting into situations where it is no longer allowed to guess because the next guess would exceed the maximum allowed guesses per day. (**Note:**

brutecreate.exe* does not evenly distribute Username/Password combinations throughout the *bruteforce.txt* file. You must do this after using *brutecreate.exe* to populate the *bruteforce.txt* file.)*.

Replacing the *bruteforce.txt* file while a sweep is in progress is *not* recommended. If you do so, PhoneSweep may repeatedly dial a phone number and hang up immediately, without completing the scan. Also, the percentage of brute force guessing that was completed will not be accurate in any report you generate. Instead, stop your scan first, replace the *bruteforce.txt* file, import the file, and Rescan the profile.

4.6.7 Using *brutecreate.exe* to customize *bruteforce.txt*

The *brutecreate.exe* utility customizes *bruteforce.txt*. To use *brutecreate.exe* open an MS-DOS prompt and go to the PhoneSweep directory. There, type the command with the following options:

```
brutecreate [combine FILEA FILEB [Flip]] | restore | clear | help
```

- ***Combine*** takes usernames from FILEA and passwords from FILEB pairs each username with each password, and appends the results to the existing *bruteforce.txt*.
  - FileA is a *.txt* file containing a list of user names (no double quotes), with each user name on its own line ending with a carriage return. You can create NULL user names by having an empty line (carriage return only).
  - FileB is a *.txt* file containing a list of passwords (no double quotes), with each user name on its own line ending with a carriage return. You can create NULL passwords by having an empty line (carriage return only).
- ***Flip*** is an optional subcommand for *Combine* that takes each username forward and reversed as the password. For example, if FILEA contains the usernames root and guest, *brutecreate.exe* will yield the additional lines for each in the form of:

"root" "root"
"root" "toor"
"guest" "guest"
"guest" "tseug"

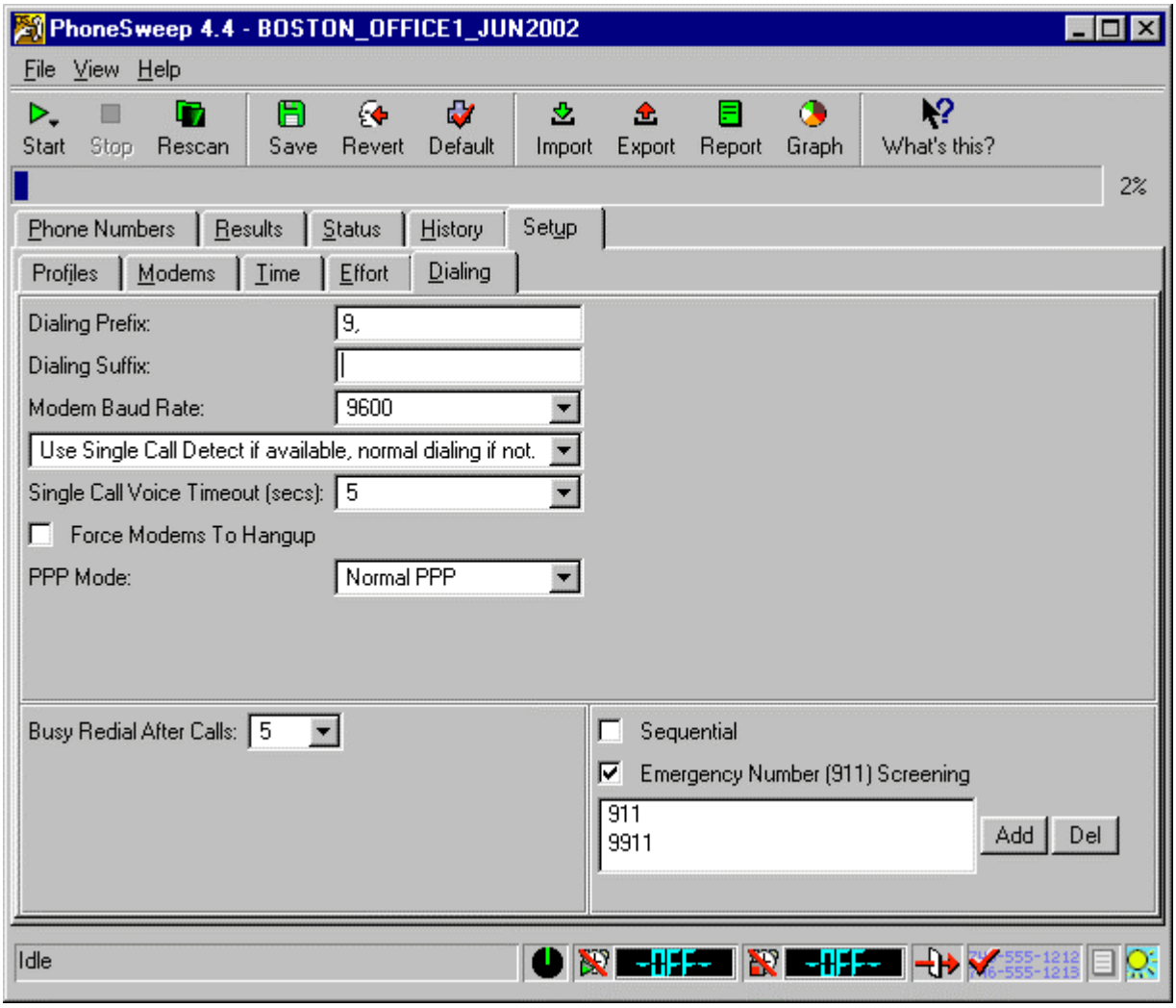
  You still must specify a FILEB for this command to work
- ***Restore*** returns *bruteforce.txt* to the default username/password combinations supplied with PhoneSweep, using *systemdefault.txt* as source.
- ***Clear*** removes all text from *bruteforce.txt*. Use this command first when you want to overwrite the existing *bruteforce.txt* file, rather than appending *brutecreate.exe*'s results to it (see Appendix F for an example).
- ***Help*** lists *brutecreate.exe* options, without actually running the program.

To add to the current *bruteforce.txt*, you must supply your own list of user names in a text file. Each user name must be on its own line, followed by a carriage return. For passwords, you can use either the supplied password source files listed above, or provide your own. As is the case with the username file, each password must be on its own line, followed by a carriage return. Sample *brutecreate.exe* input and output files are included as an example in **Appendix F: Sample brutecreate.exe Output File.**

Caution: Please be aware that increasing username/password combinations in *bruteforce.txt* will cause sweeps in Penetrate mode to be longer. Also, *brutecreate.exe* does not evenly distribute username/password combinations throughout the *bruteforce.txt* file. For these reasons, we suggest that you first sweep in Identify mode to identify modems and systems. Then create a new profile that contains only the numbers that have been identified as connecting to modems, and perform a second sweep against only those modems, or that you sweep with **Find Modems First** selected.

4.7 Setting Dialing Options

The **Dialing** sub-tab, located under the **Setup** tab, allows you to customize PhoneSweep's dialing behavior for a particular calling profile. Changes made to the **Dialing** sub-tab must be saved using the **Save** icon at the top of the PhoneSweep window.


PhoneSweep 4.4 - BOSTON_OFFICE1_JUN2002
File View Help
Start Stop Rescan Save Revert Default Import Export Report Graph What's this?
2%
Phone Numbers Results Status History Setup
Profiles Modems Time Effort Dialing
Dialing Prefix: 9,
Dialing Suffix:
Modem Baud Rate: 9600
Use Single Call Detect if available, normal dialing if not.
Single Call Voice Timeout (secs): 5
Force Modems To Hangup
PPP Mode: Normal PPP
Busy Redial After Calls: 5
Sequential
Emergency Number (911) Screening
911
9911
Add Del
Idle

The **Dialing** sub-tab allows you to:

- Activate or disable Single Call Detect
  - Use Single Call Detect if available, normal dialing if not
  - Never Use Single Call Detect
- Specify **Single Call Voice Timeout** (seconds)
- Specify **PPP mode**
- Activate or disable **Force Modems to Hangup**.
- Set dialing **Prefix** and **Suffix,** used for each number in your profile
- Set the **Modem Baud Rate**

- Set the number of times PhoneSweep will call back numbers that were busy (**Busy redial after calls**).
- Activate or disable **Sequential** dialing of phone numbers (We recommend you do not enable Sequential dialing, so PhoneSweep will dial numbers randomly)
- Enable or disable **Emergency Number (911) Screening** and modify the *Emergency Number (911) Screening list* (on a per-profile basis). (We recommend you never disable this list).
- Use PhoneSweep in environments where your dialing needs change periodically (for instance, if you need to dial the same numbers from multiple locations)

4.7.1 Setting dialing prefix and suffix

Any strings specified in these fields will be dialed before and after the phone number in each call PhoneSweep makes, respectively. The dialing prefix is intended for any access code you need to dial to reach an outside line, or other information that may change depending on your location. Either the prefix or the suffix may be appropriate to hold calling card information, but be aware that your modem has a limit on how many characters it can dial at a time. The maximum number of characters a modem can dial at a time is generally around 50, but will vary by modem. Consult the documentation for your particular modem for more information.

There are some modem commands that usually belong in the **Dialing Prefix** and **Dialing Suffix** fields instead of the phone numbers themselves, because it is more difficult to adjust these values dynamically in the phone number than the **Dialing Prefix** and **Dialing Suffix** fields. These include:

- **The W or w character** (capital or lowercase w) will cause your modem to wait for a second dial tone. If you are using a system that gives a second dial tone when you dial the code for an outside line, this pause will ensure that the actual phone number after the prefix will not be dialed prematurely.
- **The comma character** (“,”) will force your modem to pause, for most modems, for pause length defined in the S8 Register. The normal default pause for comma is 2 seconds.

4.7.2 Sequential scanning

By default, PhoneSweep dials numbers in a random order. If you wish PhoneSweep to dial numbers starting at the lowest number and ending with the highest, select the **Sequential** check box.

Using sequential scanning in conjunction with Penetrate mode can cause problems. Trying a number of brute-force username/password combinations on one modem before going on to the next number can tie the modem up for long enough to interrupt service to other users.

Maximum calls per number per day should not be used in conjunction with sequential scanning. If PhoneSweep must call numbers in order, and it reaches the allowed number of calls before it is finished with a number, it will wait. Calls to the remaining numbers in the profile will be postponed until the earlier numbers can be completed.

4.7.3 Setting PPP mode

PhoneSweep features the ability to identify and brute-force PPP systems. ToneLoc and similar programs do not have this functionality. A PPP system uses a binary protocol that is not comprehensible to text-based systems.

PPP mode is only relevant at the Identify and Penetrate levels of effort. PPP bruteforcing uses the same *bruteforce.txt* file as normal text-based bruteforcing, but PPP bruteforcing can generally make only one username/password guess per call.

There are three possible PPP identification/brute-forcing settings:

- **Normal PPP:** In this mode, if PhoneSweep attempts to identify a text protocol and fails, it will see if the remote device will respond to PPP protocol packets.
- **Never use PPP:** In this mode, PhoneSweep will not send PPP packets to attempt to identify a system that it cannot identify with text protocols.
- **PPP only (no text):** In this mode, PhoneSweep will only identify and brute-force systems which respond to PPP protocols.

4.7.4 Emergency Number (911) screening

Emergency Number (911) screening is a measure to prevent PhoneSweep from calling emergency numbers such as 911. PhoneSweep's Emergency Number (911) screening is enabled by default, and it is strongly recommended that it be left enabled in North American environments.

The Emergency Number (911) screen list defaults to 911 and 9911. However, these may not be the only numbers that connects to emergency services in your area. You should be aware of local emergency numbers in your area, and add them to the Emergency Number (911) screening list, and avoid including them in profiles. **NOTE: The Emergency Number (911) screening operates only on a per-profile basis. For every new Profile you create, you must change the Emergency Number (911) screening list.**

Sandstorm does not warrant that 911 screening will prevent all calls to emergency services.

- To disable 911 screening, click on the check box to deselect it.
- To **add numbers to the Emergency Number (911) screening list**, click on Add, type the number(s) into the dialog box that appears, and click OK. Multiple numbers may be added, separated by a comma or space.
- To **delete numbers from the Emergency Number (911) screening list**, highlight the number you want to delete, and click on Del.

4.7.5 Redialing busy numbers

The Busy Redial field sets the number of times that PhoneSweep will redial a busy number before giving up on it. A number that is always busy should be investigated further, since it may be a modem that was in use every time PhoneSweep attempted to connect to it. (Default value is 5 calls.)

4.7.6 Setting modem baud rate

The Modem Baud Rate setting can be changed to accommodate the maximum speed at which your modems will attempt to connect. **For maximum reliability, we recommend connecting at a 9600 bps (baud).** Higher baud rates do not significantly improve PhoneSweep's calling throughput, and may reduce reliability on some combinations of PC, serial I/O interface and operating systems. Many PBX systems are unable to handle high baud rates as well, especially older systems.

4.7.7 Setting Single Call Detect (SCD) mode

Normally, you should leave SCD mode enabled (**Use Single Call Detect if available, normal dialing if not**). The default attempts to use SCD on any call that is placed in both carrier mode and fax mode. We recommend that use this default setting. The other settings available are:

- **Always use Single Call Detect** triggers a modem error if PhoneSweep attempts to use SCD and fails. (We recommend you do not use this setting)

- **Never use Single Call Detect** disables SCD, and relies entirely on any Voice recognition support in your modem to avoid leaving empty voice-mail messages. (Use this setting for troubleshooting call results and in cases where it seems your modem does not seem to be using Single Call Detect).

4.7.8 Setting single call voice timeout

This timeout determines how long PhoneSweep waits for a modem or fax response after it detects that something has answered the phone. Sandstorm Enterprises recommends leaving this timeout set at its default of 5 seconds.

However, **if PhoneSweep is leaving blank voice mail messages while dialing in SCD mode,** reducing this value to 4 or 3 seconds may reduce the number of blank voice mail messages left. Too short an interval may result in PhoneSweep reporting Voice or Timeout when it would otherwise have found a modem.

Please note that with some combinations of telephone switch and voice mail configuration, it may not be possible to eliminate all blank voice messages.

After you have customized your dialing preferences, click **Save** and continue.

After you have set all the options in this section, you are ready to scan! Be sure that the hardware license management device (the "dongle") is attached to your computer's parallel or USB port before you begin your scan.

5 Sweeping

"Sweeping" describes PhoneSweep's active mode of operation: When you start a sweep, PhoneSweep actively checks the current time period against the time periods assigned to each phone number in the current open Profile. When there is a match between the Actual and assigned time periods, PhoneSweep dials that number.

5.1 Setting Up A Test Sweep

To assure yourself of the accuracy and reliability of the data collected in your sweep, you should run a test sweep against a set of numbers that reach known devices before you begin production scanning. **If you plan to use PhoneSweep at multiple sites,** we recommend that you run a test sweep at each new site, so that you can adjust PhoneSweep for variations in the local PBX and phone system as needed. A good set of numbers to call might include:

- A number known to reach voicemail
- A known disconnected number
- A data-only modem
- A fax/modem
- A fax machine
- An outside line if you will be dialing outside your phone system

Understanding how your organization's PBX and phone system operate will assist you in interpreting and evaluating the information collected in a PhoneSweep scan and aids you in making decisions based on the data collected. See **Evaluating the Results of Your Scan,** Section 10.

5.2 Before You Start Your Sweep

- Verify that the hardware license device (dongle) is connected to your computer's parallel or USB port and seated firmly.
- Disable any fax or remote access software that uses the same modems or COM ports as PhoneSweep.
- Disable your computer's screen saver.
- Disable your computer's power management software.
- Disable any virus checkers running at the time.
- Clear your computer's outgoing phone line.
- Determine make and model of both your PBX and phone system
- Determine how many seconds pass before your voice mail system picks up during each time period. Enter this time in seconds in the **Timeout in Seconds** value on the **Time** sub-tab.

- Determine how your PBX and phone system both handle unassigned and disconnected numbers. Phone systems that give a voice message for unassigned or disconnected numbers will cause these numbers to be reported as voice lines.
- Determine if you need to dial a 9 or other special codes when dialing lines outside your phone system. You can enter these as needed in either the **Prefix** or **Suffix** fields on the **Setup->Dialing** sub-tab.

5.3 Starting Your Sweep

You can start your sweep in one of two ways:

- **Click on the Start button.**
- **Select Start from the File menu** at the top of the PhoneSweep window.

When your sweep begins, the **Status** icon at the lower right of the PhoneSweep window will become active. The **Status** icon looks like a small radar screen ( ). There may be a noticeable pause before PhoneSweep actually begins to dial, especially if you have a large list of phone numbers and have made many calls already.

5.4 Starting and Ending a Sweep Automatically

You can use either the **Time Periods** settings or the **Scheduled Stop and Start times** to dictate when PhoneSweep will begin scanning.

Under normal conditions, you would start a sweep, knowing that PhoneSweep will not dial any number unless the current time period matches any time period assigned to given number. Controlling the sweeps by setting the Business Hours, Blackout Hours, and Weekend time periods usually suffices.

In some cases, however, PhoneSweep's time periods may not be sufficient to describe the desired sweeping behavior. For instance, you may want to start a scan at 8:00 PM on a Friday night, but want to leave the office at 5:00 PM. Or, you may want to stop a scan at 5:30 AM on a Monday morning, but not want to come in to work at that time to actually stop the PhoneSweep scan.

Scheduled start and stop allows you to specify a time to start or stop a sweep. Click and hold the **Start** button to see the **Scheduling Options** menu, or access it as a submenu from the **File->Start** menu option. Click on **Schedule Start** to set a start time for the sweep, and **Schedule Stop** to set a time for the sweep to end.

If you don't schedule a stop, the sweep will stop when it is finished or the time period changes to one in which there are not phone numbers set to be dialed. Scheduled times are displayed in the status bar at the bottom of the PhoneSweep screen (when no start or stop is scheduled, the indicators display "**--OFF--**"at the bottom of the User Interface).

To disable the scheduled events, choose **Cancel Scheduled Start** or **Cancel Scheduled Stop** on the **Scheduling Options** menu. When you restart PhoneSweep or switch profiles, scheduled events for that profile are canceled, but can be re-enabled with **Schedule Start** and **Schedule Stop**. The set times are retained so that you don't have to re-select them.

Please note that whenever you start a sweep, PhoneSweep is constantly checking the actual time against the time period(s) assigned to each phone number. No number will be dialed unless the current time is within the time period(s) assigned to that phone number

5.5 Sweeping for ISDN devices

When scanned, most ISDN modems will respond to incoming analog calls. Some ISDN modems, such as the Motorola Bitsurfer, will respond only to ISDN data or ISDN data-over-voice calls. To find such modems, scan first with an ISDN modem, and then follow up by scanning with a normal modem.

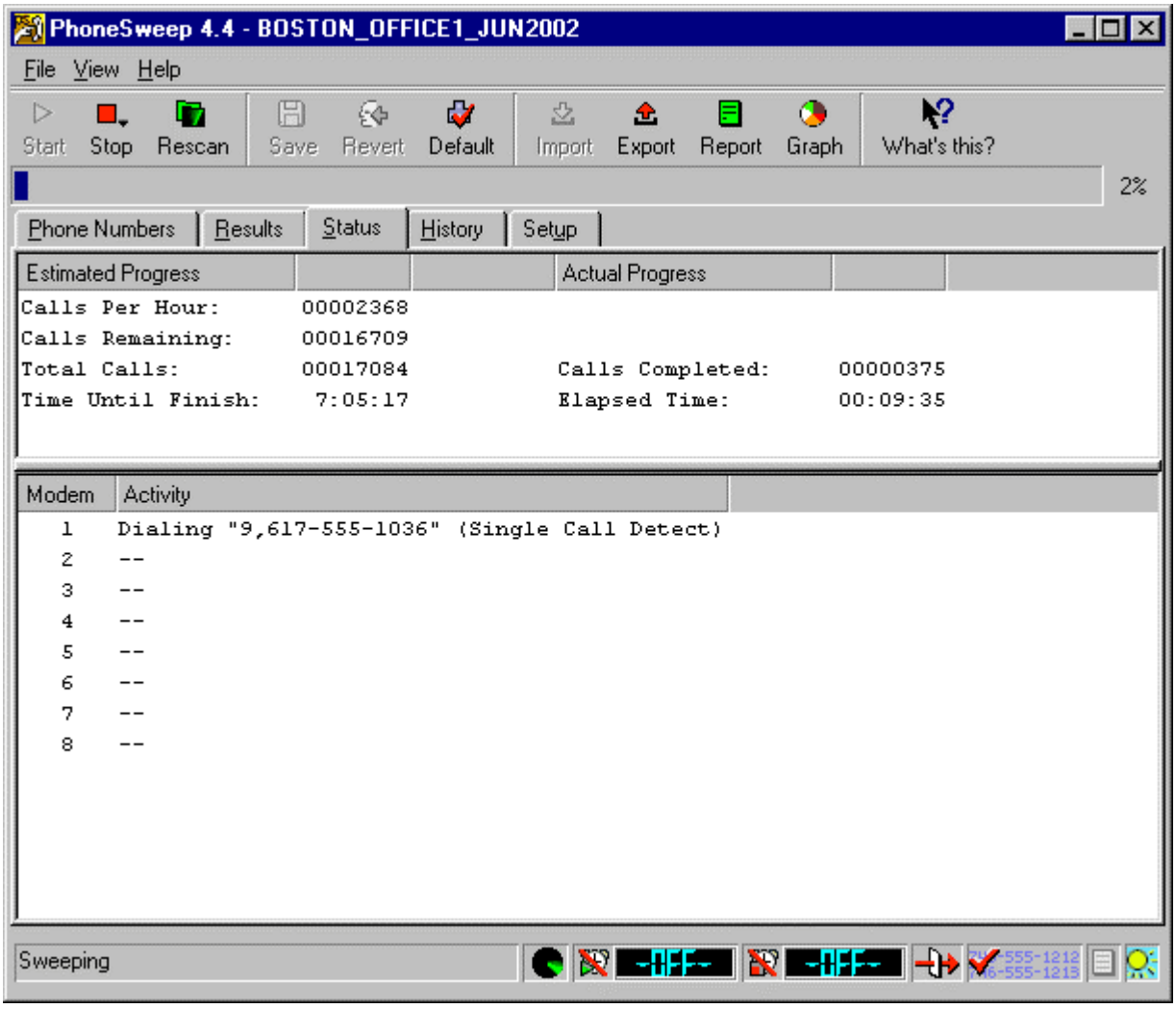
- For scanning purposes, we are not aware of any ISDN modems that support Single Call Detect. To both take advantage of SCD mode and find ISDN devices, it is best to scan a profile twice:
    - Once in SCD mode with a Zoltrix or other SCD-capable modem, and then
    - Scan a second time for "Modems only" with an ISDN modem (we recommend the U.S. Robotics Courier Imodem.

If you choose to you can do a scan by calling first in data mode (Find Modems Only) and then in fax mode (Find Fax Machines Only) with a hybrid analog/ISDN modem. However, please note this will take twice as many calls as scanning the profile twice with the two different modems. It will also inconvenience the users more, because of the lack of rapid voice ID and because a human will hear loud beeping if they answer the phone.

5.6 Monitoring Your Sweep in Real Time

The **Status** tab shows the real-time status of a sweep in progress (estimated and actual), as well as the current status of each modem as it progresses through a sweep. The real-time data displayed on the **Status** tab are:

- Estimate of the time required to complete the current sweep
- The rate at which PhoneSweep is progressing through the profile
- How much progress PhoneSweep has made
- What each of your modems is currently doing



5.6.1 Estimated Progress

The Estimated Progress area of the **Status** tab shows the estimated progress for the current sweep. PhoneSweep estimates:

- The rate at which PhoneSweep is executing the sweep in **Calls Per Hour**
- The number of **Calls Remaining** (yet to be made.)
- The **Total Calls** it expects the sweep will require
- **Time Until Finish**

These estimates will usually change rapidly at the beginning of a sweep. More specifically, *PhoneSweep will almost always overestimate the work required*, especially in Penetrate mode. The initial estimates in Penetrate mode assume that all numbers reach devices that can be brute-forced, and that PhoneSweep can guess only one username/password combination per call. **Calls Per Hour** starts at 60 calls per hour per active modem, which is subsequently updated during the sweep by the actual average number of calls made per hour per active modem.

5.6.2 Actual Progress

The Actual Progress area of the **Status** tab displays:

- The number of phone calls completed
- Elapsed time spent sweeping. This measures only time spent sweeping, not the total time elapsed since the Start button was clicked.

5.6.3 Modem Status

The bottom of the **Status** tab displays information about what the modems are currently doing. For example, your modems may be

- Idle. "Modem Idle" simply means the PhoneSweep is not dialing, and does not indicate that the program is not responding.
- Dialing a remote phone number. If the modem is dialing, the number that is being dialed will appear next to the "Dialing" message.
- Trying to identify a computer system attached to a remote modem.
- Guessing a username/password combination.
- Hanging up.

5.6.4 Why might a modem become "disabled"?

If any modem is not selected on the **Modem** sub-tab, there will be two dashes next to that modem's number.

If a modem's Activity changes to "Disabled," one of the following may be true:

- **The modem may not be powered on.**
- **The modem may not be receiving a dial tone.** Make sure that your modems are plugged into a working phone line, and that modems requiring an analog phone line have such a line. Also determine if anyone may have called into the line.

PhoneSweep may be unable to communicate with the modem. Check the list of Error Messages for the **Status** tab on page 130 for help diagnosing possible problems. PhoneSweep counts communications errors with each modem. After several errors in succession from a modem, PhoneSweep will disable it. Stopping and starting the sweep will clear the error count and PhoneSweep will try to use the modem again. If the modem continues to receive errors, have your phone system technician check the line and the PBX. The **History** tab may provide more information about errors that have disabled a modem. Click on the **History** tab for more detailed information on a specific modem's errors.

If a modem appears hung or disabled and you want to reactivate it, try using the **Reset Modem** option by right-clicking on the modem. This option is available on the **Status** and **Modems** tabs.

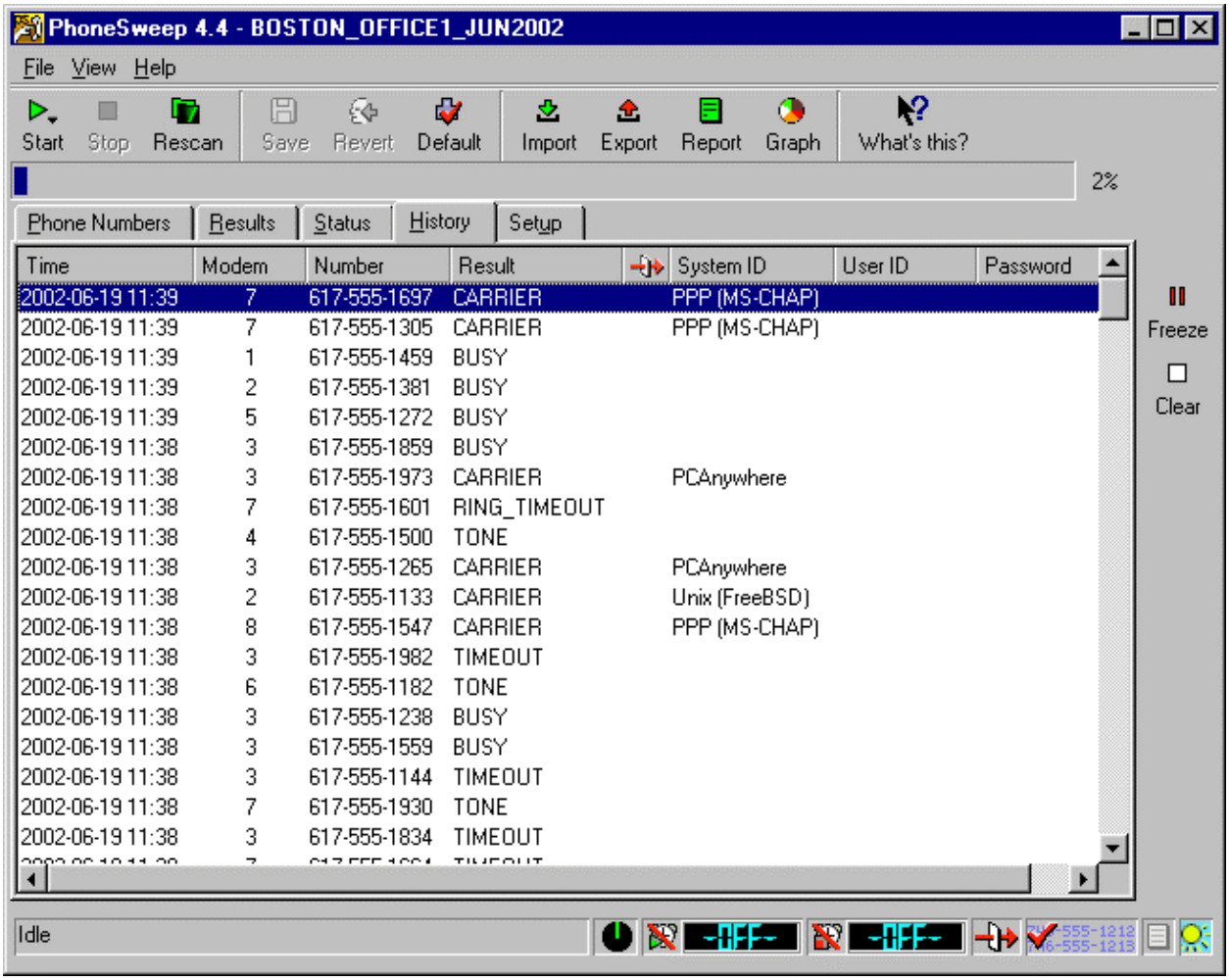
The display on the **Results** tab also continuously updates as the sweep progresses.

5.7 Monitoring Recent Events: The History Tab

The **History** tab displays the 250 most recent calls and their results. The **History** tab is updated in real-time as PhoneSweep dials numbers during a sweep. You can clear and freeze the real-time display as needed.

The **History** tab shows you:

- The date and time a call was made.
- The modem that placed the call.
- The number that the modem called.
- The result of the call.



The **Freeze/Thaw** button stops and starts the real-time display. Clicking on the button will toggle it between these two states. When the button is toggled to **Freeze**, the call history is stored in a buffer until the button is toggled to **Thaw**. When the button is changed from **Freeze** to **Thaw**, the **History** display will show the last 250b events at that current moment in time. If more than 250 events happen while the display is frozen, some may not appear when the History is thawed. Whether or not the display is frozen, PhoneSweep will continue to sweep.

The **Clear** button clears the screen display of its current contents.

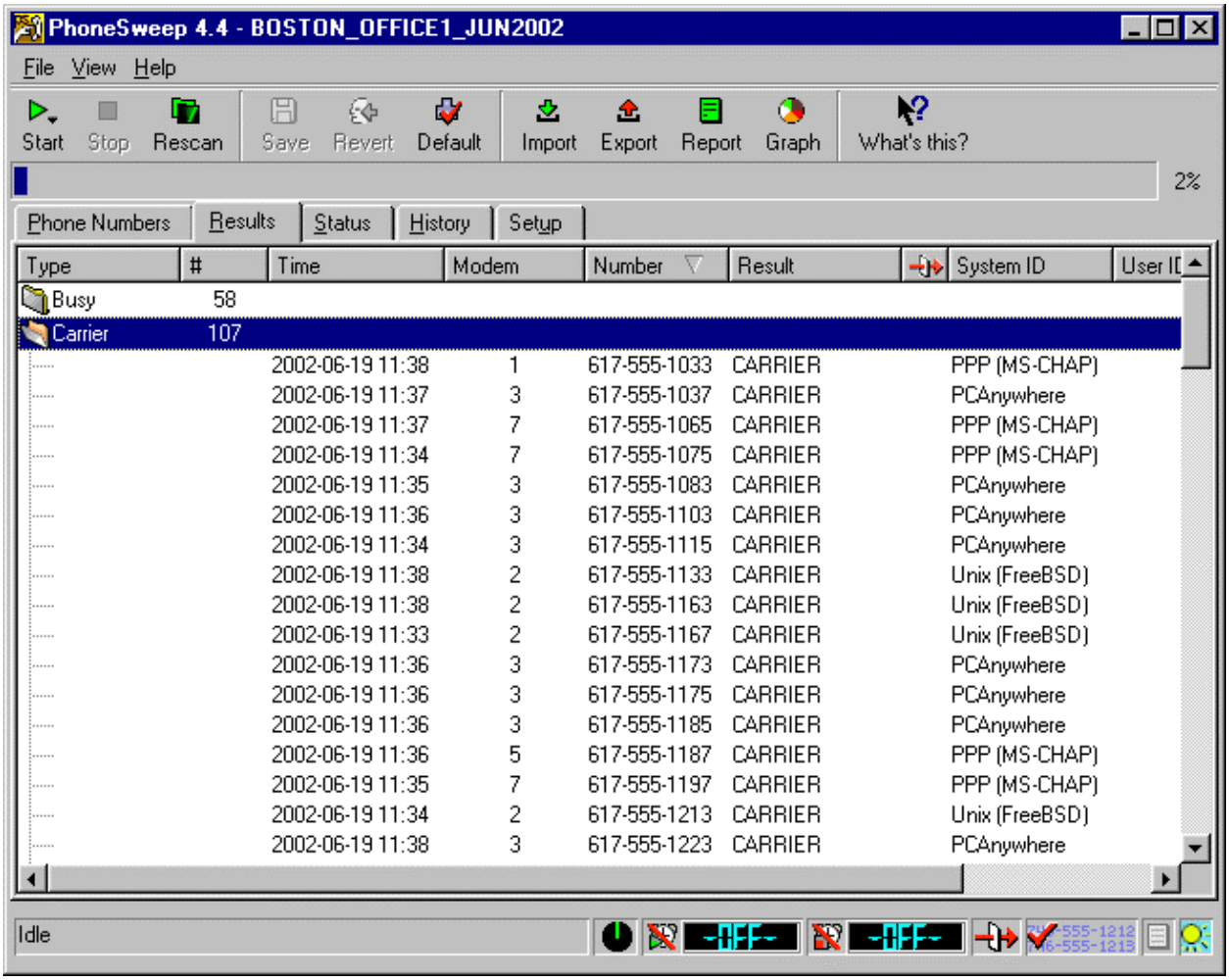
Right-clicking on an entry in the History Tab will give you the option to see a **Call Detail** of the event (displayed in a separate pop-up window), or to search within the list contents using the **Find…** feature. Searching will begin at the current entry.

5.8 Viewing Your Results

The **Results** tab summarizes the responses PhoneSweep has received from numbers it has dialed. Each folder icon on the display contains a list of phone numbers that have given responses in the indicated category. If no phone numbers have elicited a particular category of response, this is indicated by a small icon of a telephone handset. Like the **Status** tab, the display on the **Results** tab is also updated in real-time as a sweep progresses.

Clicking on a folder toggles back and forth between showing and not showing the contents of the folder.

Right-clicking on an entry gives you options to expand and collapse folders, see a Call Detail of the event (displayed in a separate pop-up window), or to search within the list contents using the **Find…** feature. Searching will begin at the current entry.


PhoneSweep 4.4 - BOSTON_OFFICE1_JUN2002
File View Help
Start Stop Rescan Save Revert Default Import Export Report Graph What's this?
2%
Phone Numbers Results Status History Setup
Type # Time Modem Number Result System ID User ID
Busy 58
Carrier 107
2002-06-19 11:38 1 617-555-1033 CARRIER PPP (MS-CHAP)
2002-06-19 11:37 3 617-555-1037 CARRIER PCAnywhere
2002-06-19 11:37 7 617-555-1065 CARRIER PPP (MS-CHAP)
2002-06-19 11:34 7 617-555-1075 CARRIER PPP (MS-CHAP)
2002-06-19 11:35 3 617-555-1083 CARRIER PCAnywhere
2002-06-19 11:36 3 617-555-1103 CARRIER PCAnywhere
2002-06-19 11:34 3 617-555-1115 CARRIER PCAnywhere
2002-06-19 11:38 2 617-555-1133 CARRIER Unix (FreeBSD)
2002-06-19 11:38 2 617-555-1163 CARRIER Unix (FreeBSD)
2002-06-19 11:33 2 617-555-1167 CARRIER Unix (FreeBSD)
2002-06-19 11:36 3 617-555-1173 CARRIER PCAnywhere
2002-06-19 11:36 3 617-555-1175 CARRIER PCAnywhere
2002-06-19 11:36 3 617-555-1185 CARRIER PCAnywhere
2002-06-19 11:36 5 617-555-1187 CARRIER PPP (MS-CHAP)
2002-06-19 11:35 7 617-555-1197 CARRIER PPP (MS-CHAP)
2002-06-19 11:34 2 617-555-1213 CARRIER Unix (FreeBSD)
2002-06-19 11:38 3 617-555-1223 CARRIER PCAnywhere
Idle
-OFF-
-OFF-

5.8.1 Timestamps

Each time a phone number is called and classified, it is placed in a folder along with the date and timestamp of the call. If successive calls to that phone number yield different results, that phone number will appear in more than one category with each instance labeled with the unique date and time of the call. Except for the **Penetrated** category, multiple calls to the same number that produce the same result, (e.g. several Busy calls) will result in only one call timestamp being listed. All successful penetrations will be displayed.

5.8.2 Categories of results

Busy	The phone number was busy.
Fax	A fax machine answered the remote phone number.
Screened	The phone number was not dialed because the number matched our test for an emergency number.
Timeout	PhoneSweep did not receive a carrier signal within the designated wait interval.
Ring Timeout	No person or device answered the phone before the specified number of rings (requires "remote ring" support in your modem).
Voice	A person, an answering machine, or a voicemail message answered the phone.
Tone	PhoneSweep heard a second dial tone or some other tone.
Carrier	A modem answered the call.
Untrained Carrier	Either a fax or a modem answered the call; the type of device was undeterminable. Some (usually non-recommended) modems may report this result.
Penetrated	In Penetrate mode, PhoneSweep successfully logged in to an answering device. In Identify mode, PhoneSweep found a device which did not require a username/password to log in.
No Facsimile	No fax machine was detected at this number. This is only an intermediate result, and should change to another state as the sweep is completed.

The following categories can be confusing and are therefore explained in more detail:

- **Numbers classified as Fax:** In general, numbers classified as Fax only appear if a scan was done in fax mode or in fax and data mode. However, some physical fax machines (not fax/modems) will respond with a fax tone on a data scan, and be reported as Fax. (Note: Xerox Copier machines that are Fax capable and that use Super Fax speeds (Super Group III) may be misidentified in Connect mode as Fax/Modems, but correctly identified as Fax machines in Identify mode, where PhoneSweep does not rely on sound of signal alone. The Super Group III Fax communication uses compression to achieve high transmission speeds and may sound like data transmission).
- **Numbers classified as No Facsimile:** All PhoneSweep has been able to determine about a number so far is that it is not a fax machine. When more information is learned about a number, it is removed from this category. There should be no numbers in this category in a completed sweep.
- **Numbers classified as Carrier:** The list of Carrier numbers will include PhoneSweep's best guess as to the identity of the computer system attached to the remote modem when PhoneSweep is run in Identify or Penetrate mode. These guesses will not appear in real time. To view the identities of contacted systems, reload the profile using the **Profile** tab.
- **Numbers classified as Penetrated:** The list of Penetrated numbers will initially contain the date and time stamp, the phone number called, and the username/ password combination that successfully penetrated the remote system. After reloading the profile, as with Carrier numbers, the system identification will be listed between the phone number and the successful username/password combination.

5.8.3 Identification of remote systems

PhoneSweep can only identify computer systems for which Sandstorm Enterprises has determined correct response strings (presently over 450 systems). If you encounter a system that PhoneSweep cannot identify, please contact Sandstorm. We will incorporate the response strings into the next version of PhoneSweep.

For a complete list, please see List of Identified Systems in Appendix I.

5.9 Rescanning a Profile

In some situations, you may want to rescan a previously scanned set of numbers such as when you want to be sure that no new modems have been added to the system since the last sweep. Or perhaps you previously made a scan that detected insecure modems, and want to make sure that those modems have been removed.

The **Rescan** function makes a clone of the current profile (or the Profile you have highlighted on the **Profiles** sub-tab), preserving the same set of phone numbers and scanning options with a new name, but without call results information from the previous scans.

To rescan the current Profile, click the **Rescan** button on the menu bar. To rescan a different profile, go to the **Profiles** sub-tab and highlight (select) the profile you want to rescan, then click the **Rescan** button.

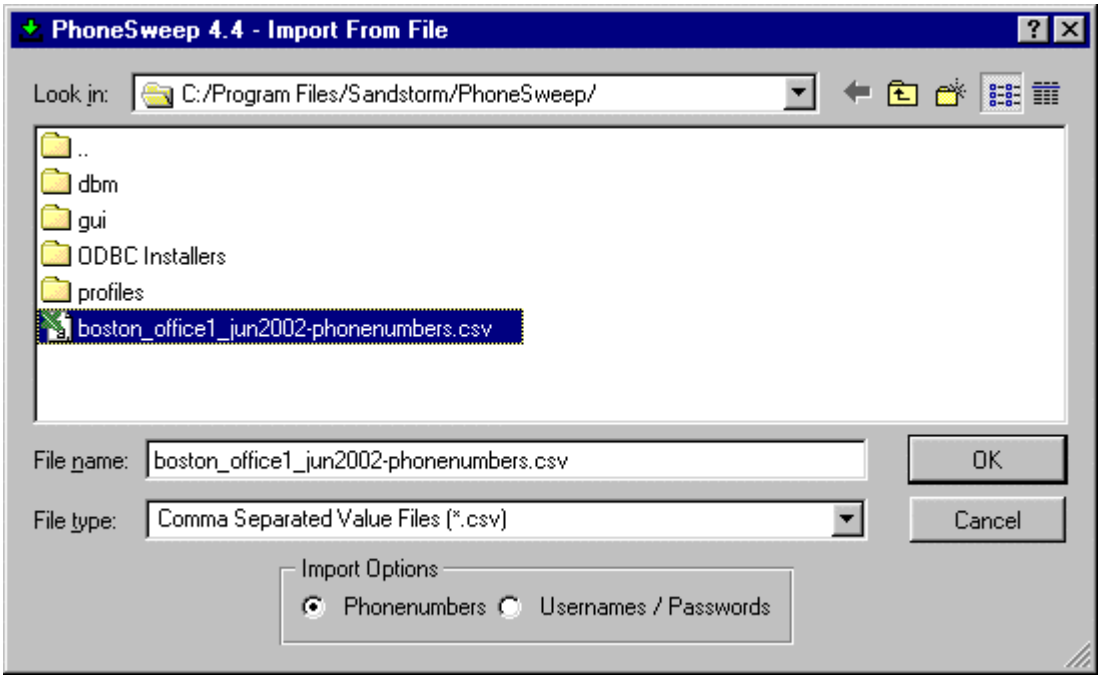
You will be prompted to name for the new profile. Once you have entered a profile name, **Rescan** creates the new Profile and opens it for scanning. You can then click the **Start** button to begin the new sweep.

Normally you will not want to use the **Rescan** button until the first sweep has been completed, but it is possible to **Rescan** an unfinished scan if required. If this has been done, the unfinished scan can be completed later by switching to it and clicking **Start.**

6 Importing and Exporting Data

There are times when entering information manually into PhoneSweep would require a prohibitive amount of work. Therefore, PhoneSweep allows you to import pre-existing sets of phone numbers and brute-forcing information.

6.1 Importing Phone Number Lists



Before importing a file containing lists of phone numbers into PhoneSweep,

- Make sure that the file is formatted as specified in the following section,
- Make sure that the time period codes are set appropriately in the file.

Click on the **Import** button to import a file containing a list of phone numbers. When the **Import Dialog** box appears, enter the name of the file containing the list of phone numbers, select the "Phone numbers" Import Options, and then click OK.

6.1.1 Formatting imported phone numbers

A file containing phone number/time period code pairs to be imported must be in text format ("MS-DOS Text with line breaks", in Microsoft's terms). Each phone number and time period code pair must be by itself on a line terminated by a carriage return/linefeed, and formatted in one of the following patterns (do not include the angle brackets):

- <phone number> <*Tab*> <time period code> <*CRLF*>
- <phone number> <*Comma Space*> <time period code> <*CRLF*>
- <phone number> <*Space Space*> <time period code> <*CRLF*>
- "<phone number>"<comma>"<Timeperiod code>"<CRLF>

- <phone number> <*CRLF*>

Note: Because there is no time period given in the last example, the default import time period will apply (See "Default Time Period" below.).

The phone number field can include the characters **1 2 3 4 5 6 7 8 9 0 ( ) . - # x X a A b B c C d D**. Phone numbers and time periods can contain quotes; quotes will be stripped out by the import function and changed to spaces. This also means that the format "phone number", "time period code" will be imported correctly. The quotes will be changed to spaces, creating the comma-space separator, and other additional spaces will be stripped out by the import function. Examples are as follows:

555-1000

555-1200<TAB> 28

555-1127<Comma Space>28

555-1666<Space Space>28

"555-1299"<Comma Space>"28"

Note: If last line of your .csv or .txt file is a space. it may cause errors.

Note: If the comma is to be used as a Pause when dialing a given Phone Number, please enclose the comma and Phone Number together in Double Quotes, and enclose the Time Period in Double quotes, separating both by another comma: "555-1000,3","28"

6.1.2 Importing Phone Numbers with associated Notes

To import associated notes with each phone number, you **must import the time period code** as well. Otherwise, PhoneSweep will give you "Incorrect Time Period" error on import. To include associated notes, use one of the following 3 formats:

- <phone number> <*Tab*> <time period code><*Tab*>Note <*CRLF*>
- <phone number> <*Comma Space*> <time period code> <*Comma Space*><Note> <*CRLF*>
- "<phone number>"<comma>"<Timeperiod code>"<*comma*>"<Note>"<CRLF>

6.1.3 Time Period codes

The time period code is a number that encodes the time period(s) during which a phone number should be called. Whether or not you change the time period values from their default values using the **Time** tab, the *codes* remain the same.

The time period codes (in decimal) are:

Time Period(s)	Value
Business Hours	2
Outside Hours	12
Weekends	16
Business Hours & Outside Hours	14
Business Hours & Weekends	18
Outside Hours & Weekends	28

Business Hours, Outside Hours, & Weekends (Any time period)	30

A sample file that would dial the numbers 555-1212 during business hours, 555-1213 during any time period, and set 555-1214 to use the default import value would be:

```
555-1212 <Tab> 2
555-1213 <Tab> 30
555-1213
```

Note that the <*Tab*> is an ASCII Tab formatting character (control-I, decimal value 9).

6.1.4 Default Import Time Period

Phone Sweep supports a default time period, which is applied to any numbers imported without an accompanying time period value. If you are importing lists of phone numbers from other applications, typically a PhoneSweep time period will not be included, and the default time period will be applied during the import.

The default value is set to **Dial During Any Time Period**, which corresponds to a value of 30 when using the **Default Import Time Period** option. You can change the default value via the **Dialing** sub-tab, or by creating an entry for DEFAULT-IMPORT-TIMEPERIOD variable in the [vars] section of the *phonesweep.ini* file. (See Section 4.4.5, **Setting time periods for imported phone numbers**)

Caution: If you do not explicitly specify a time period code, you should avoid creating phone numbers that include double spaces or a comma followed by a space. PhoneSweep will interpret them as separator characters and not import the phone number correctly.

In general, the use of comma-space combinations inside phone numbers in input files can cause problems. If you want to put comma-space combinations in your phone numbers, we recommend the use of tab-separated lines with explicit time period values.

6.2 Importing Brute Force Information

A list of username/password combinations is used for guesses in Penetrate mode when PhoneSweep attempts to break into remote systems. PhoneSweep stores this list internally for each profile, but initially populates the internal database from the file *bruteforce.txt*. Although a starter list is provided with PhoneSweep, you will probably need to customize *bruteforce.txt* to reflect username/password pairs appropriate for your site. PhoneSweep offers the following options for changing the *bruteforce.txt* file:

- Import Username/Password pairs from either your own custom files or *systemdefault.txt*, which contains default Username/Password pairs for many systems.
- Enter Username/Password pairs via the Setup-> Effort tab. When you are finished, you can export the internal Username/Password pairs into a new file.
- Use *brutecreate.exe* to combine usernames and passwords from separate files to add to *bruteforce.txt* (*brutecreate.exe* can also reset *bruteforce.txt* to its default values from *systemdefault.txt*).
- Edit the *bruteforce.txt* file directly.

6.2.1 Formatting imported Username/Password pairs

To import a file containing a list of Username/Password pairs, click on the **Import** button. When the **Import Dialog** box appears, enter the name of the file containing the list of phone numbers, select the "Usernames/Password" Import Options, and then click OK.

For PhoneSweep to be able to use imported username and password files, the following formatting must be used: The username and password are each delineated by double quote characters. Any unquoted text on a line is ignored. Each username/password pair is on a single text line ending in a Carriage Return/Line Feed sequence ("MS-DOS Text with line breaks" in Microsoft's terms). For example:

```
"root"    "toor"
"system"  "manager"
"guest"   "guest"
```

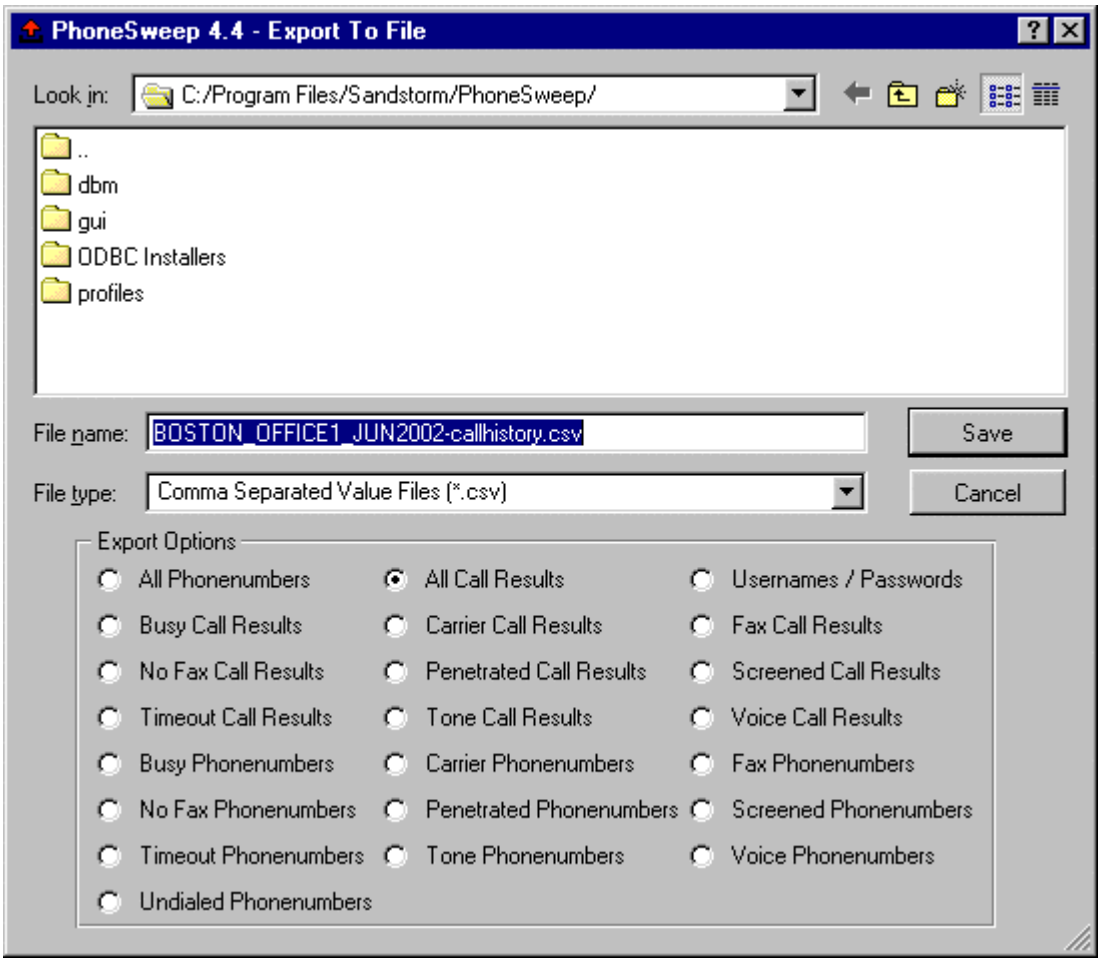
If you are making bruteforce username/password guesses against Microsoft NT RAS servers where a Domain must be specified, this must be entered as a prefix to the username, with a '/' as a separator, i.e. "Payables/pay" "me".

(Note for users of earlier versions of PhoneSweep: PhoneSweep's format for username/password entries has changed for version 4.0. The format from earlier versions of PhoneSweep [using <*Tab*> as the separator] will be supported for at least two more releases, but we recommend converting any existing files as soon as possible*.)*

Save the file of username/password combinations you have created, and copy or rename it to *bruteforce.txt* in the main PhoneSweep directory. By default, this is C:\Program Files\Sandstorm\PhoneSweep. If you specified a different path during installation, use that instead.

For more information on using *bruteforce.txt* when PhoneSweep is in penetrate mode, see Section 4.6.6, **The bruteforce.txt file**.

6.3 Exporting Data



6.3.1 Exporting Call History

To export a comma-separated list of the results of all calls PhoneSweep has made, select the **History** tab and click on the **Export** button. This will create a file in the following format (call parameters will replace the angle-brackets and text within them):

"<phonenumber>","<timestamp>","<Faxcall>","<Callresult>","<idtext>","<Bruteresult>","<username>", "<password>","<CID>","<ParentCID>","<Continuation>"

Here is an example of call history output via **Export**:

```
"555-1000","1999-03-16 17:55:43","2","4","Simulator","111","0","","", "0","0"
```

This indicates a call made to 555-0000 at 17:55 on March 16, 1999. Values for other fields are explained below.

Possible values of Faxcall

Fax call	1
Data call	2
Both fax and data call	3

SCD mode call	4
SCD mode specifically trained to listen for Fax	21

In the above example, *Faxcall*=2, indicating a data call was placed. *Faxcall* values other than those listed above indicate combinations of call types, and are the sum of the values for the call. For instance, a call made in SCD mode (4) that is both a fax and a data call (3) will have the value 7.

Possible values of Callresult

Busy	1
Screened	2
Ring timeout	3
Seconds-based timeout	4
Voice	5
Fax	6
Tone	7
Carrier	8
Continued carrier call	9
No fax machine	10
Untrained Carrier	11

In the above example, *Callresult*= 4; the call resulted in a seconds-based voice timeout.

Continued carrier calls (*Callresult*=9) mark second and third (or greater) brute-force username/password guessing attempts during a single call. Although they are not actually separate calls, they are logged separately in the call history database to make processing easier. They are not listed as separate calls under the **Results** tab or in RTF (rich text format) reports.

No Fax machine (*Callresult*=10) calls are separate calls, but are not exported, reported, or listed under the **Results** tab unless there are no other call results for that phone number except Busy.

The idtext field

The *idtext* field is text, giving PhoneSweep's best guess as to the remote system's identity. The default identification is "Unknown", which appears even in non-carrier calls. In the above example, *idtext*= "Simulator", that is, a call made in PhoneSweep's simulator mode.

The Bruteresult field

The *bruteresult* bit field gives the result of a username/password guess. If no bruteforce guess was made, the value of the bit field will be 0.

If the *bruteresult* field has a value of 1, then an unsuccessful guess was made, but no specific information could be gleaned from the error message. Therefore, either the username or password was bad. This case is reported as **Bad Username or Password.**

Otherwise, the *bruteresult* field is generated by a username result and a password result. The codes are:

Bad_Username	2
No_Username	4
Good_Username	8
Bad_Password	16
No_Password	32
Good_Password	64

The username and password fields

The username and password fields record which username and password were used in a brute-force guess. If no brute-force guess was made (*bruteresult* = 0), then the username and password will be empty strings.

The CID field

The CID (Call ID) is used as a primary key by PhoneSweep. This number is guaranteed to be unique within a profile.

The Parent CID field

The **parent CID** is the CID of the original (Carrier) call to a system that is being brute-forced. The Parent CID field is 0 on all calls except Carrier Continued calls. Since PhoneSweep records the username and password guessed on calls, it records additional username/password guesses as additional calls.

The Continuation field

The **Continuation** field indicates the order of Carrier Continued calls so that they can be sequenced easily. Calls that are not Carrier Continued calls have a continuation number of 0. The first Carrier Continued call will have a Continuation of 1, the second will have a Continuation of 2, and so on.

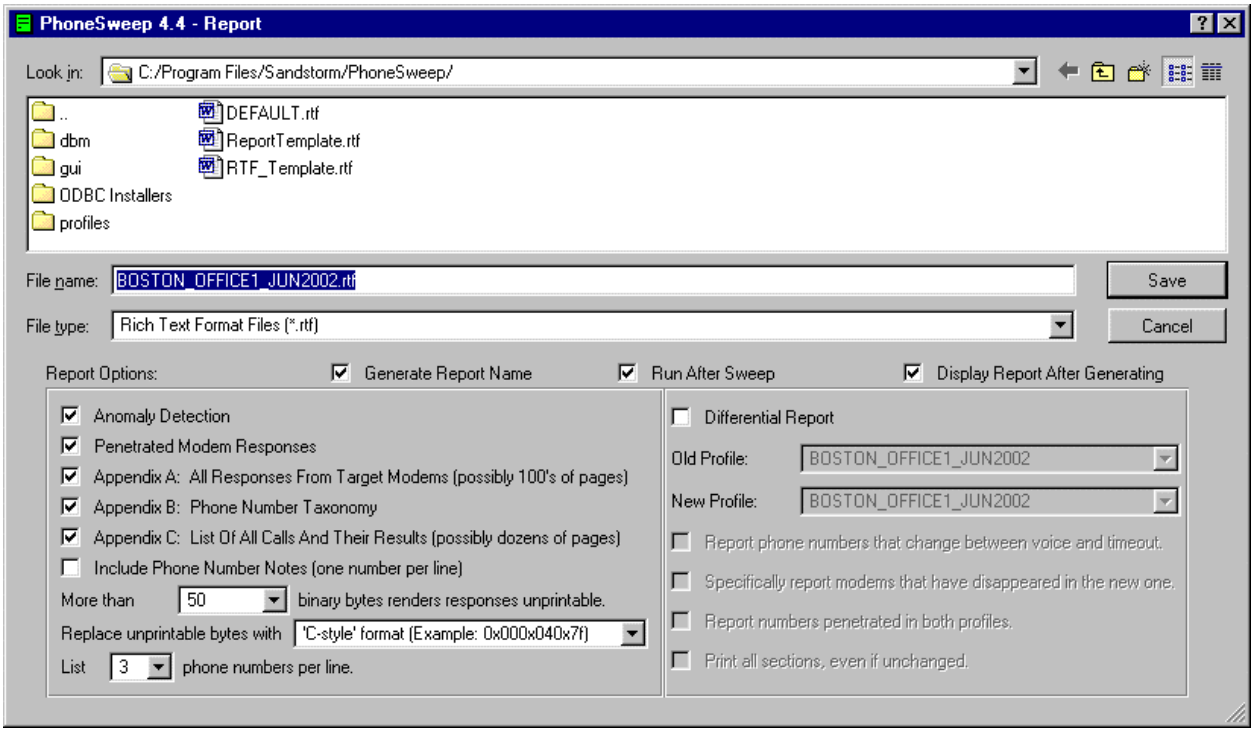
7 Generating PhoneSweep Reports

The **Report** feature takes PhoneSweep call results and organizes them into an easily readable form that highlights problems and vulnerabilities. PhoneSweep reports are clearly formatted, easy to review and suitable for printing or importing into other documents.

PhoneSweep can generate two basic types of reports: a report of what happened in one profile and a report that compares two profiles and indicates all the differences found (Differential Report). This section deals with generating standard PhoneSweep reports. Refer to Section 8, **Differential Reporting**, for information about Differential Reporting.

PhoneSweep generates reports as **Rich Text Format (RTF) files**, compatible with Microsoft Word and other word processors. You can use RTF-compatible word processors to view, modify or print PhoneSweep reports. Microsoft's WordPad (standard with Windows operating systems) will also read a PhoneSweep report, but will not properly display or print more complex formatting elements, such as tables.

7.1 Selecting Standard Report Sections



To generate a **Standard Report**, call up the **Report Dialog** box, either by clicking the **Report** button in the button bar at the top of the PhoneSweep window, or selecting **Report** from the File menu to generate the report. You may choose to run the report after the next sweep instead of immediately, and display the report automatically after generating it, by checking the appropriate boxes.

The **Report** dialog box gives you the option of deciding what information you want in your report. By suppressing or including various sections, you can omit irrelevant data and generate a report more quickly. Some of the sections may run to hundreds of pages for a long sweep, so be sure to review the contents before printing PhoneSweep reports.

The **Optional Sections** are formatted to be read from beginning to end. The **Appendices** are not intended to be read from start to finish; they are included as reference material.

7.1.1 Anomaly Detection

The Anomaly Detection section lists any anomalies that PhoneSweep found during checks on remote modems. Anomalies are inconsistent responses from one call to the next; they often indicate an unauthorized or misconfigured modem.

For example, two calls to the same phone number might yield a modem (Carrier) on the first call and Voice on the second. This could be an unauthorized modem that is only activated some of the time. Another phone number might connect with Carrier on most calls, but report Timeout one out of four times. This may indicate a faulty modem.

The Anomaly Detection section may take a substantial amount of time to generate, since it is crosschecking responses against each other, but it does not generate a lengthy section in the report. We recommended that you include the Anomaly Detection section in most reports, because it often shows serious problems with security or reliability.

The Anomaly Detection section is included by default. To exclude the Anomaly Detection section from the report, click the check box to deselect it.

7.1.2 Penetrated Modem Responses

The Penetrated Modem Responses section of the PhoneSweep report prints the entire buffer received from each modem that was successfully penetrated. These buffers contain useful information about what computer system is connected to the penetrated modem. Unless PhoneSweep has managed to penetrate a large number of modems, this section is likely to be reasonably short.

The Penetrated Modem Responses section is included by default. To exclude this section from the report, click the check box to deselect it.

7.1.3 Appendix A: All Responses From Target Modems

Appendix A includes the full response buffer from every Carrier call. This appendix is useful for getting information about systems that PhoneSweep was unable to identify.

If you have a large number of modems to test or a large username/password database, Appendix A can easily run to hundreds of pages. *Check the length of reports including Appendix A before sending them to a printer*.

Because of its potential length, **Appendix A is excluded from the report by default**. To include it, click in the appropriate check box.

7.1.4 Appendix B: Phone Number Taxonomy

Appendix B lists PhoneSweep's best guesses as to the nature of the system that answered each call. The information is sorted by phone number. If a phone number responds in multiple different ways to multiple calls, each response will be included in the list. If PhoneSweep was able to correctly guess any usernames and passwords, they will be included in Appendix B with the phone number.

If there are systems that PhoneSweep does not identify, please contact Sandstorm. We are interested in obtaining data so future versions of PhoneSweep can identify those systems. In many cases, the appropriate section of Appendix A will contain all the information necessary for engineering PhoneSweep to identify that system.

Appendix B is turned on by default.

7.1.5 Appendix C: List of All Calls and Their Results

Appendix C simply lists in chronological order every call that PhoneSweep made during the sweep. Included is the response made by the remote phone number and any brute-force username/password guessing, successful or unsuccessful.

Appendix C may large, especially if you are scanning a large profile or if you have a long username/password list. Depending on the output device and font selected, approximately 50 calls will be listed on each page of printout

Appendix C is turned off by default.

7.1.6 Binary bytes and replacing unprintable characters

Responses from remote modems are sometimes hundreds of characters long. These features allow you to instruct PhoneSweep to avoid printing long binary strings in modem responses, or display them with different numeric formats.

7.2 Customizing Your Report Template

PhoneSweep reports are generated using a template called *ReportTemplate.rtf* in the top-level PhoneSweep directory. *ReportTemplate.rtf* is a Rich Text Format file. You can view *ReportTemplate.rtf* with Microsoft Word or other RTF viewers, such as WordPad. We do not recommend that you use WordPad to edit *ReportTemplate.rtf*.

ReportTemplate.rtf is the master template used to generate PhoneSweep reports. Therefore, any changes made to *ReportTemplate.rtf* will be reflected in all PhoneSweep reports you subsequently generate.

By editing *ReportTemplate.rtf*, you can:

- Change the formatting of PhoneSweep reports
- Re-arrange PhoneSweep report sections
- Add or remove explanatory text from PhoneSweep reports

Make a backup copy of *ReportTemplate.rtf* before editing it. If you forget to make a backup copy of *ReportTemplate.rtf* and want to return to the default template, reinstalling PhoneSweep will restore the original template. Reinstalling PhoneSweep will not affect any of the profiles you have created. You can also copy the default template off the PhoneSweep CD-ROM.

The *ReportTemplate.rtf* file consists of sections and variables.

7.2.1 Report Sections

Report sections mark areas in the report where PhoneSweep enters specific blocks of information, such as the list of all phone calls made.

The *ReportTemplate.rtf* file marks report sections by a triad of characters: a pound sign, a number, and another pound sign. For example, #7# marks the Anomaly section.

The following table lists each report section marker and an explanation of the information contained in that particular report section. The report section markers do not need to be placed in any particular order within the *ReportTemplate.rtf* file.

Section Marker	Section Content
#7#	Print the Anomaly section. This section contains phone numbers that responded in odd ways.
#9#	Print a list of phone numbers that PhoneSweep successfully Penetrated.
#10#	Print modem responses from systems that were successfully Penetrated.
#12#	Print all phone numbers that responded with Carrier.
#13#	Print all phone numbers that were always Busy.
#14#	Print all phone numbers that responded with Second Dial Tone.
#15#	Print any areas where the sweep was not completed.
#17#	Print all responses from all modems that PhoneSweep connected to. This may be an extremely long list.
#19#	Print the classification of each phone number PhoneSweep dialed.
#21#	Print the results, sorted by time, of every call PhoneSweep made.
#25#	Print whether PhoneSweep scanned for data modems, fax machines, or both.
#26#	Print the phone numbers associated with all systems that PhoneSweep was able to identify, as well as their identification strings.
#27#	Print all unidentified phone numbers that responded with Carrier, as well as any partial identification information collected.
#28#	Print all phone numbers that responded with a Fax signal.
#29#	Print all responses from modems that could not be identified by PhoneSweep.
#30#	Print the note associated with the profile in question.
#31#	Print all phone numbers dialed, without call results.

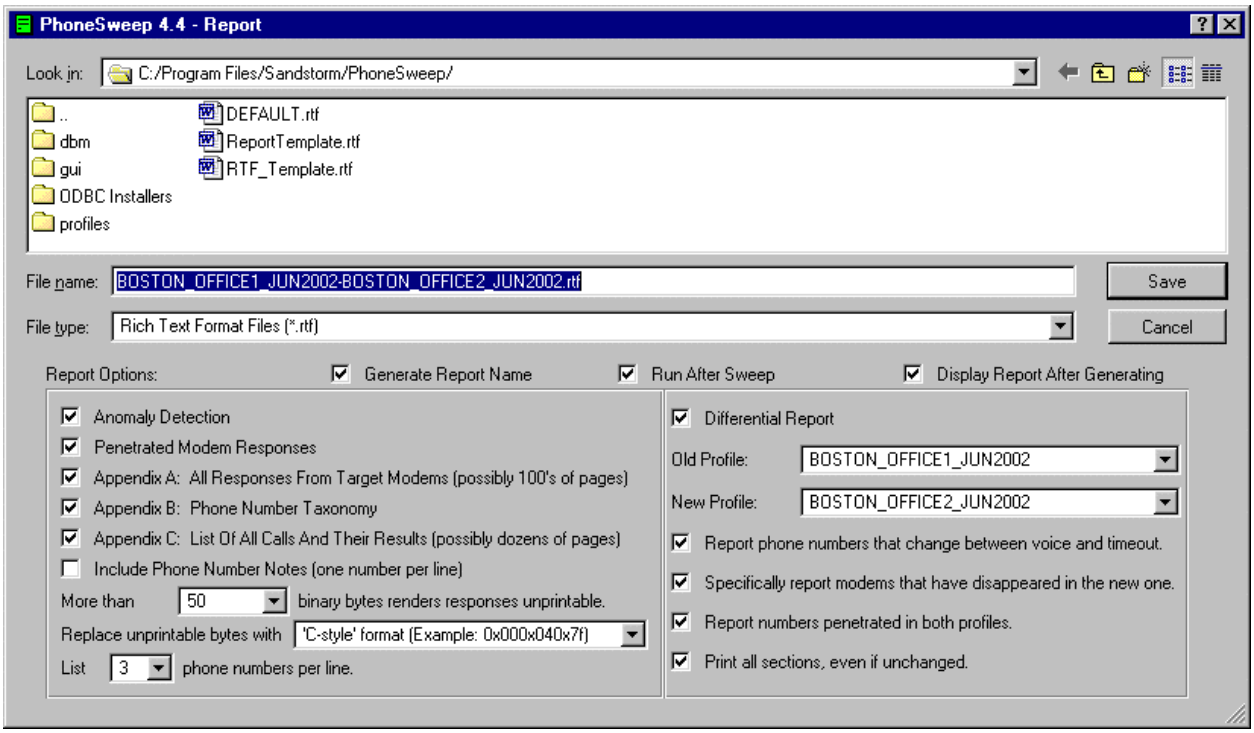
7.2.2 Report variables in ReportTemplate.RTF

A report variable in *ReportTemplate.rtf* is replaced by a value when the report is generated. The following table contains a list of the report variables and their values.

Variable	Value
%ALLN%	Total number of phone numbers assigned to dial.
%ALLPC%	Either 0% if no numbers were dialed or 100% if any numbers were dialed.
%BFPC%	Percentage of username/password guessing completed.
%BN%	Total number of phone numbers that were always Busy.
%BPC%	Percentage of dialed numbers that were always Busy.
%CALLS%	Total numbers of calls made by PhoneSweep.
%CN%	Total number of phone numbers that responded with Carrier.
%CNALLPC%	Either 0% if no numbers responded with Carrier, or 100% if some numbers did.
%CPC%	Percentage of dialed numbers that responded with Carrier.

%DATEGEN%	The date and time the report was generated.
%DATESTART%	The date and time PhoneSweep started scanning.
%DATESTOP%	The date and time PhoneSweep stopped scanning.
%DN%	Total number of phone numbers dialed in data mode (checked for Carrier).
%DFN%	Total number of phone numbers dialed in fax mode.
%DFPC%	Percentage of numbers dialed in fax mode.
%DPC%	Percentage of assigned numbers dialed in data mode.
%ETIME%	Total time spent sweeping phone numbers.
%FN%	Total phone numbers called where a fax machine responded.
%FPC%	Percentage of dialed numbers that responded with fax.
%ICN%	Phone numbers with Carrier attached to systems that were identified
%ICPC%	Percent of Carrier numbers for which the system could be identified.
%IPNN%	Penetrated phone numbers for which the system was identified.
%IPNPC%	Percentage of Penetrated numbers for which systems were identified.
%ON%	Total phone numbers that responded with a second dial tone.
%OPC%	Percentage of dialed numbers that responded with second dial tone.
%PNN%	Total phone numbers that were penetrated
%PNNALLPC%	0% if no systems were penetrated, or 100% if some were.
%RN%	Total phone numbers that rang enough times to time out.
%RPC%	Percentage of phone numbers that rang long enough to time out.
%SCDN%	Total number of phone numbers dialed in Single Call Detect mode.
%SN%	Total phone numbers that were screened.
%TN%	Total phone numbers with standard timeout.
%TPC%	Percentage of dialed numbers with standard timeout.
%UCN%	Phone numbers with carrier that could not be identified.
%UCPC%	Percentage of phone numbers with Carrier that was not identified.
%UPNN%	Phone numbers that were penetrated but could not be identified.
%UPNPC%	Percentage of penetrated numbers that were not identified.
%VN%	Total phone numbers that responded with Voice.
%VPC%	Percentage of dialed numbers that responded with Voice.

8 Differential Reporting


PhoneSweep 4.4 - Report
Look in: C:/Program Files/Sandstorm/PhoneSweep/
..
dbm
gui
ODBC Installers
profiles
DEFAULT.rtf
ReportTemplate.rtf
RTF_Template.rtf
File name: BOSTON_OFFICE1_JUN2002-BOSTON_OFFICE2_JUN2002.rtf
Save
File type: Rich Text Format Files (*.rtf)
Cancel
Report Options:
Generate Report Name
Run After Sweep
Display Report After Generating
Anomaly Detection
Penetrated Modem Responses
Appendix A: All Responses From Target Modems (possibly 100's of pages)
Appendix B: Phone Number Taxonomy
Appendix C: List Of All Calls And Their Results (possibly dozens of pages)
Include Phone Number Notes (one number per line)
More than 50 binary bytes renders responses unprintable.
Replace unprintable bytes with 'C-style' format (Example: 0x000x040x7f)
List 3 phone numbers per line.
Differential Report
Old Profile: BOSTON_OFFICE1_JUN2002
New Profile: BOSTON_OFFICE2_JUN2002
Report phone numbers that change between voice and timeout.
Specifically report modems that have disappeared in the new one.
Report numbers penetrated in both profiles.
Print all sections, even if unchanged.

Differential reporting is a PhoneSweep feature that produces a report listing the differences between two calling profiles. This is useful for ensuring that threats have been removed and identifying threats that may have appeared since a previous sweep.

To generate a **Differential Report**, call up the **Report Dialog** box, either click the **Report** button in the button bar at the top of the PhoneSweep window or select **Report** from the **File** menu to generate the report. Then click on the **Differential Report** checkbox at the center right of the dialog box.

The **Differential Report** section of the **Report Dialog** box allows you to:

- Specify the two profiles to be compared.
- Select optional information to include in the differential report.

When you have made your desired selections, click the OK button. There will be a delay while the differential report is generated.

8.1 What information is in a differential report?

The heading of the differential report lists the profiles being compared and shows settings of various important parameters in each profile. The body of the differential report lists phone numbers for which the results of the second scan (the “new profile”) differed from the results from the first scan (the “old profile”), sorted by category. An example appears in **Appendix H: A Sample Differential PhoneSweep Report**. The differential report will not include the information from a single-sweep report; varying the options listed on the left side of the **Report** dialog box (except for the **Display Report After Generating** checkbox) will not affect the content of the differential report.

8.1.1 Heading

The heading of the differential report contains the following information:

- The date and time when the differential report was generated.
- The name of the old calling profile.
- The name of the new calling profile.
- Each scan's level of effort.
- The devices that each scan was configured to search for (modems, fax machines, or both).
- The value of Busy Redial in each profile.

8.1.2 Engineering Summary

The Engineering Summary section lists differences between the results of the two profiles. These may include:

- Phone numbers called in one sweep but not in the other
- Systems penetrated in one sweep but not in the other
- Modems, faxes or second dial tones found in one sweep but not the other
- Systems identified differently in the two profiles.

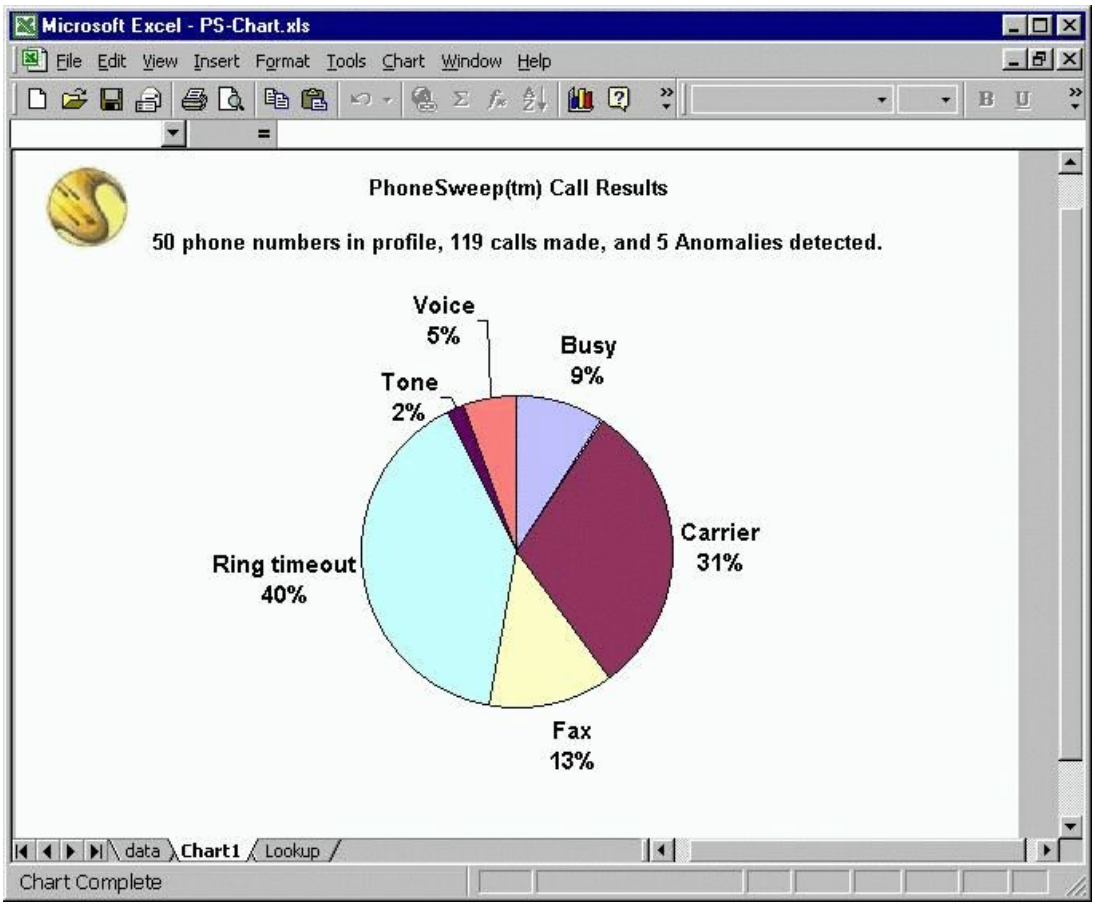
8.1.3 Full Call History Change Report

The Call History Change Report includes information on specific changes in call results, sorted by phone number. This will highlight any phone numbers whose response changed from one sweep to another, i.e. from Carrier to Timeout, Busy to Voice and so forth. Some of these will be authorized configuration changes, which should be checkable against other data sources. Others will be caused by random events: Voice on one call and Timeout on another usually indicates a person who simply happened to be at their desk during one scan. The differences that remain after eliminating the intentional and random changes are usually worth further investigation.

9 Graphing Call History Results

If you have Microsoft Excel 2000 installed, the results of the current profile can be sent to Excel automatically to display a pie chart of the call results. Select the **Graph** button after or during a sweep. There will be a delay while Excel starts. When it does, you will be prompted to enable Macros. Click to enable Macros; then after the spreadsheet loads, click on the large yellow button entitled "Click here to create a pie chart of your sweep results." If you don't have Excel 2000 installed, or you don't have any call history results to graph, an error message will be displayed.

Sample PhoneSweep Chart



Like any other Excel graph, the graph produced can be edited. For example, if you want to change the title, you can click on it and edit it. You can also change the graph to a column chart by clicking on the pie chart and going to "Selected Data Series" under Format. For more information on editing the chart, see your Excel 2000 manual.

The **Graph** button also exports your PhoneSweep call results into Excel spreadsheets, eliminating the need to use PhoneSweep's Export button to do so. In the lower left corner of the chart, the raw call history data generated by your sweep will appear under the "data" tab. The summary data, including the final call result assigned to each phone number appears under the "lookup" tab. You can save these sheets in Excel 2000 and use them like any other Excel spreadsheet. For an explanation of the data fields, see Section 6.3.1, **Exporting Call History**.

10 Evaluating the Results of Your Scan

The following chart shows the normal results of a scan, sorted by type of device, level of effort, and whether or not Single Call Detect (SCD) was used.

10.1 Expected Sweep Result Charts

The 5 charts below detail the call results (and interpreting some misidentifications) for each type of line, when scanning both without and with Single Call Detect (SCD) for:

- Fax and Modems together
- Just Faxes
- Just Modems

The line types are:

- Voice
- Fax
- Modem
- Fax/Modem
- Second Dial Tone

The call result types are:

- **Carrier** = This line has a modem.
- **Fax** = This line has a fax machine.
- **NO_Facsimile =** This line is not a fax machine.
- **None** = No Call Made
- **Timeout** = either line did not pick up (Ring Timeout) or line was not identifiable after pickup. It did not respond as **Fax** (when looking for Fax) or as a **Carrier** (when looking for Carrier).
- **Tone** = There is a second tone on this line.
- **Voice** = Voice (person or voice recording responded). When using NO SCD, voice lines are identified as Timeouts.

The results below are those found during in-house testing of PhoneSweep; however, some telephone systems will yield different results.

Please note: All line types initially have listed "Unknown" System ID next to them. If PhoneSweep determines that a line is a) carrier (modem) and is b) able to identify the system or device on the other side, then Unknown is changed to the identified System name.

10.1.1 Voice Line Sweep Results

Call Type	Connect		Identify		Penetrate	
	NO SCD	w/ SCD	NO SCD	w/ SCD	NO SCD	w/SCD
Fax & Carrier 1st Call	Timeout	Voice	Timeout	Voice	Timeout	Voice
2nd Call	NO_Facsimile	None	NO_Facsimile	None	NO_Facsimile	None
Fax only	NO_Facsimile	NO_Facsimile	NO_Facsimile	NO_Facsimile	NO_Facsimile	NO_Facsimile
Modem only	Timeout	Timeout	Timeout	Timeout	Timeout	Timeout

If Voice lines consistently identify as Seconds-Based timeout, try increasing the Single Call Detect Voice Timeout on the options Setup-> sub-tab.

10.1.2 Fax Line Sweep Results

Call Type	Connect		Identify		Penetrate	
	NO SCD	w/ SCD	NO SCD	w/ SCD	NO SCD	w/ SCD
Fax & Carrier 1st Call	Timeout	Fax	Timeout	Fax	Timeout	Fax
2nd Call	Fax	Timeout	Fax	Timeout	Fax	Timeout
Fax only	Fax	Fax	Fax	Fax	Fax	Fax
Modem only	Timeout	Timeout	Timeout	Timeout	Timeout	Timeout

Fax Misidentifications: Some Faxes will misidentify at the connect level as Fax/Carrier. If this occurs, please retry those faxes at the Identify level of effort where an actual Fax Group 3 protocol handshake occurs. We suspect that faxes that misidentify at the Connect level only

Some faxes will continue to misidentify as Fax\Carrier at the Identify and Penetration level of efforts. We suspect that these Faxes either have undeveloped or undocumented features, or, have modem features for optional modem connections that can be fully added later.

10.1.3 Modem Line Sweep Results

Call Type	Connect		Identify		Penetrate	
	NO SCD	w/ SCD	NO SCD	w/ SCD	NO SCD	w/ SCD
Fax & Carrier 1st Call	Carrier	Carrier*	Carrier, System if Identified	NO_Facsimile	Carrier, Username/ Password	NO_Facsimile
2nd Call	NO_Facsimile	NO_Facsimile	NO_Facsimile	Carrier, System if Identified	NO_Facsimile	Carrier, Username/ Password
Fax only	NO_Facsimile	NO_Facsimile	NO_Facsimile	NO_Facsimile	NO_Facsimile	NO_Facsimile
Modem only	Carrier	Carrier	Carrier, System if Identified	Carrier, System if Identified	Carrier, Username/ Password	Carrier, Username/ Password

Carrier Misidentifications: Occasionally during the beginning and end of a sweep with multiple modems, some Carrier lines will misidentify as voice lines if two modems attempt to call the same number at the same time.

10.1.4 Fax/Modem Line Sweep Results

Call Type	Connect NO SCD	Identify w/ SCD	Brute-force NO SCD	Line Type w/ SCD	Connect NO SCD	Identify w/ SCD
Fax & Carrier 1st Call	Carrier	Fax	Carrier, System if Identified	Fax	Carrier, Username/ Password	Fax
2nd Call	Fax	Carrier	Fax	Carrier, System if Identified	Fax	Carrier, Username/ Password
Fax only	Fax	Fax	Fax	Fax	Fax	Fax
Modem only	Carrier	Carrier	Carrier, System if Identified	Carrier, System if Identified	Carrier, Username/ Password	Carrier, Username/ Password

10.1.5 Second Dial-tone Sweep Results

Call Type	Connect NO SCD	Identify w/ SCD	Brute-force NO SCD	Line Type w/ SCD	Connect NO SCD	Identify w/ SCD
Fax & Carrier 1st Call	Timeout	Tone	Timeout	Tone	Timeout	Tone
2nd Call	NO_Facsimile	None	NO_Facsimile	None	NO_Facsimile	None
Fax only	NO_Facsimile	NO_Facsimile	NO_Facsimile	NO_Facsimile	NO_Facsimile	NO_Facsimile
Modem only	Timeout	Timeout	Timeout	Timeout	Timeout	Timeout

Misidentifications can happen for second Dial-tones. This is largely a result of the modem's interpretation of certain sounds: certain types of rings and line noise can cause the modem to think there is a second dial-tone after initial call pick up. When this occurs, further investigation must be done by hand (telecommunications personnel) in order to verify whether a given line has been misidentified or if the line has been compromised.

Currently, certain results do not report as anomalies in the PhoneSweep Report. They are:

- **Fax/Busy:** Lines were identified as Fax lines, but were busy when PhoneSweep tried to test them as being carrier (modem) too).
- **Voice/timeout**: Two modems attempted to call the same number close together in time.

10.2 Characteristics of telephone systems that can affect the results of a scan

Telephone switching systems often differ in subtle ways that can affect the results of your scan and how some categories of detection results should be interpreted. Therefore, you should be aware of both how your particular phone system operates and various ways in which a phone system can affect your scan or even give incorrect results. Understanding how your phone switch works helps interpret the results of your scan and also aids in troubleshooting any problems that may arise during a scan.

In some cases, a phone switch can make a click when a call is handed off to another component or an external trunk. Sometimes, PhoneSweep may interpret this click as the call being answered. If so, PhoneSweep may misidentify calls. When PhoneSweep senses that the call has been picked up, it starts a timer. If PhoneSweep does not get tones from a modem or fax machine before the timer runs out, PhoneSweep hangs up and records VOICE, although in fact the call may not even have been answered yet. On the other hand, if PhoneSweep misinterprets a click from the phone switch as the call being picked up and the next sound it encounters is a tone, PhoneSweep may misidentify the number as reaching a fax machine.

Numbers that time out must be considered with reference to the way unassigned numbers are handled on your phone system. On some systems, numbers that are not assigned give busy signals when called, or they may all be routed to voicemail, a recorded message, or special tones. More information on interpreting numbers that time out is given in the next section.

You should also be aware of any differences in how internal and external calls are handled, as well as any potential differences between dialing by extension only and dialing with the full number. Some telephone systems produce tones when dialing internal extensions but not external numbers. Others use a different type of ring when calling internal versus external extensions, or while dialing by extension vs. using the entire number. Also, if you require a prefix or extension to dial outside your organization, make sure that it is only dialed when appropriate. If you have modified your *phonesweep.ini* file to automatically include a dial-out prefix, this can cause problems if you create a profile containing internal extension numbers.

Before you begin production scanning, you should do a test sweep in which you call numbers known to reach the devices that you are looking for or may encounter in the course of a sweep. This is especially important if you are using PhoneSweep at multiple sites (see Section 5.1, **Setting Up A Test Sweep**).

10.3 Threats posed by various devices and situations

10.3.1 Data-only modems

Any data modem that can be called from outside is a potential vulnerability. If the modem or attached computer doesn't require a password to log in, it is a severe threat and should be removed or secured immediately. If PhoneSweep in Penetrate mode succeeds in executing a brute-force attack against that modem and logging into the attached computer, the threat is less severe: Your course of action will depend on your assessment of the relative weakness of the username/password that PhoneSweep used.

10.3.2 Fax/modems

A fax/modem is a device that is capable of both fax and data communications. A fax/modem will be reported as Fax by PhoneSweep running in fax mode, and as Carrier by PhoneSweep running in data mode. In SCD mode, PhoneSweep will report a number that reaches a fax/modem first as Fax and subsequently as Carrier.

All of the caveats for data-only modems apply to fax/modems. In practice, fax/modems pose a greater security risk than data-only modems. A user who installed the hardware and software only to receive faxes may not be aware that the fax/modem can also answer incoming data calls and thus not perceive a need to secure it.

10.3.3 Fax machines

Users who have been allocated analog lines to receive faxes may also use the line for dialup access with an unauthorized modem. If such a modem is not secured, it will pose a security risk.

10.3.4 Combination answering machine/fax

The main threat from a combination answering machine/fax is that an unauthorized modem will find its way onto the line. The answering machine/fax does not pose a threat in and of itself.

10.3.5 Numbers that report “VOICE”

Numbers that report VOICE are most likely human-answered phones or voicemail, and generally do not pose a security threat, although they should be investigated if it is not known who is responsible for a particular line. It is possible that a VOICE response could be a combination answering machine/fax machine or a fax machine that otherwise plays a recorded message before sending fax tones. If a number that reports as VOICE has been disconnected or is unassigned, contact your telephone system personnel to find out if your phone system automatically provides a voicemail message for disconnected or unassigned numbers.

10.3.6 Fax machine issues

As Faxes approach higher transmission speeds with compression (Super G3 Faxes which run up to 36.6Kbs using the JBIG compression), we are beginning to see where Fax tones can be confused with Data tones. Thus, in Connect mode, where PhoneSweep only listens for the tone and then hangs up, we sometimes see a Fax misidentified as a carrier. However, when in Identify mode, where PhoneSweep actually communicates with devices, using the appropriate protocol handshakes, PhoneSweep will correctly identify such machines as Fax only. .

In the case where certain makes and models of Fax Machines report as Fax/Carrier (Modem) in Identify or Penetrate Levels of Effort, we believe these machine contain either undeveloped/undocumented features; or “ready-to-use” features so that new features, such as a modem, can be added after purchase.

That said, you might still want to check out the Fax machine to make sure that it is only Fax-capable, and not a fax/modem.

10.3.7 Incorrectly configured software

It is possible, although uncommon, for PhoneSweep to hang a system that it calls. This is not merely an annoying side effect of running PhoneSweep; if PhoneSweep hangs a system that it calls, you have discovered a serious vulnerability. Denial of Service is a serious threat, and systems that crash or hang when called without the proper protocol represent a Denial of Service vulnerability. Improperly configured remote access software may hang or leave the line off-hook for a long time if an incoming call doesn't proceed as expected, leaving the service unavailable. For example, some versions of pcAnywhere take a few minutes to reset if they are called without a login attempt, during which time calls will not be answered and the dialup will be unavailable.

Also note that some versions of popular remote access software, such as Carbon Copy or pcAnywhere, do not require a password by default. It is important to educate users about the necessity of securing all modems with passwords.

10.3.8 Numbers that consistently time out

Your response to numbers that consistently time out depends on what you hope to accomplish with the PhoneSweep scan and your knowledge of how your particular phone system is configured. Typically, you should check to see if a line that times out is actually in use, or if there is a problem in your wiring or PBX configuration.

If all currently assigned phone numbers should go to voicemail, it would be reasonable to assume that numbers that time out in SCD mode are not assigned. Alternatively, on some switches unassigned

numbers give busy signals. In this case, numbers that time out may represent phones that are misconfigured (they don't go to voicemail, or have been call-forwarded outside the organization).

If you get Timeout for valid lines and do not get it on some other lines, check the lines that don't get Timeout. You can call a known disconnected number to see what response to expect from your switch.

Data-only remote access lines normally pick up on the first ring, but combination voice/fax/data equipment may not pick up until the second or fourth ring. A number that always times out could conceivably be a modem configured to not pick up until it has seen more rings than PhoneSweep is configured to try. This is uncommon and is less likely to be a significant security risk, since measures that make it harder for PhoneSweep to find modems also make it harder for an attacker to find the modems.

10.3.9 Default passwords

Default usernames and passwords are a common vulnerability in network and data communications equipment. Even when the manufacturer documents them, many equipment installers neglect to change them. Your *bruteforce.txt* file should include default usernames and passwords for the systems on your site, in order to catch instances where the defaults have not been changed to something more secure.

10.3.10 Second dial tones

A second dial tone is a dial tone in response to a code entered on the telephone (a "telephone extender"). These often give access to restricted calling privileges, such as long-distance calling. If attackers find a number that is a telephone extender, they may be able to make long distance calls that will be billed to your organization.

10.3.11 Numbers that are always busy

Numbers that are always busy warrant further investigation, because they might be connected to a modem that was in use for the whole period of the scan.

10.4 Mis-identifications

Some situations and devices have been identified as generating false identifications. In each case it is usually some non-standard or un-expected behavior. All mis-identifications should be reported to PhoneSweep Technical Support for eventual inclusion in the manual or PhoneSweep itself.

10.4.1 Fax machines known to generate mis-identifications

Certain fax machines have been known to generate Fax/Modem misidentifications, despite being just fax machines without applied modem options. Some fax machines generate mis-identifications only at the Connect level of effort due to the sounds they generate. Some fax machines generate mis-identifications at all levels of effort due to some aspect of their design that results in an exchange of modem protocols. In detail, the causes for mis-identifications are as follows:

- Super Group III Protocol, which is marketing speech for Faxes that achieve the upper limits of Fax Group III Protocol speeds by using compression. At the Connect level of effort this may sound like a modem tone. (Connect level of effort only).
- Undocumented features or non-standard fax modem design (Older Fax machines especially - All levels of effort).
- Optional "Modem Add on" features, that though not activated, may still have the modem components installed.(All levels of effort).

Faxes known to generate mis-identifications at Connect level of effort only:

- Xerox Work Center Pro 657
- Xerox DC 332 (Data copier with Fax (Super Group III) and networking addons
- Potentially other Xerox Data copiers with Fax addons that use the Super Group III protocols (as reported at one site - all their Super Group III Xerox machines generated Mis-Identifications at Connect level of effort).

Faxes known to generate mis-identifications at all levels of effort:

- Brother Fax, model unknown (Old machine)
- Cannon L 770
- Cannon L785
- Muratec F120
- Ricoh FAX2800L
- Ricoh FAX4500L

10.4.2 Situations that may generate false Penetration results

Some systems or system behaviors may generate false penetration results - and may even indicate a security risk (Systems that do not disconnect after 3 failed attempts allow hackers to continue bruteforcing attempts).

In some instances PhoneSweep may not recognize that it has penetrated a system as it does not recognize the system response for a successful penetration. In other instances, a system recycling back to the initial welcome or other banner after 3 failed login attempts may generate a false penetration report. (This is a security issue as then the system allows someone to continue in their penetration attempts during the same call).

The best way to view PhoneSweep's entire communication in Penetrate level of effort is to generate a report with the **Appendix A** option selected.

10.4.3 Other situations that generate mis-Identifications

Some other situations, such as line noise, may generate mis-identifications. These should be looked at on a case-by-case basis. Please see **Appendix C: PhoneSweep Troubleshooting Guide** for further details.

11 Customizing PS Defaults Using the PhoneSweep.INI file

If you want to change the default values that PhoneSweep uses when it creates a new profile, modify the *phonesweep.ini* file. The *phonesweep.ini* file is a standard Windows INI file. There are currently two sections, the **[globals]** section and the **[vars]** section. All variables are in the form NAME=VALUE, each on a line by itself. Any variable not present in the file will be set to its standard PhoneSweep default, and illegal lines will be ignored. If the value you specified is not being set correctly, verify that the variable is correctly spelled and that the value is appropriate.

Example: Although all modems are by default disabled when PhoneSweep starts, you could enable your first and second modems on COM1 and COM5 with the following *phonesweep.ini* file:

```
#
# PhoneSweep initialization file
#
[globals]
; Do not put your own comments
; in the [globals] section.
; They will be deleted.
FAX-INIT-STRING-1=
FAX-INIT-STRING-2=
FAX-INIT-STRING-3=
FAX-INIT-STRING-4=
MODEM-COM-1=Y
MODEM-COM-2=Y
MODEM-COM-3=N
MODEM-COM-4=N
MODEM-FORCE-HANGUP=N
MODEM-INIT-STRING-1=ATE1Q0V1
MODEM-INIT-STRING-2=ATE1Q0V1
MODEM-INIT-STRING-3=ATE1Q0V1
MODEM-INIT-STRING-4=ATE1Q0V1
MODEM-PORT-1=1
MODEM-PORT-2=5
MODEM-PORT-3=3
MODEM-PORT-4=4
MODEM-SPEAKER-1=1
MODEM-SPEAKER-2=1
MODEM-SPEAKER-3=1
MODEM-SPEAKER-4=1

[vars]
SEQUENTIAL SEARCH=N
```

The **[globals]** section sets per-machine variables.

Type	Default	Global Variable Name	Legal Variable Values
String		FAX-INIT-STRING-1	Any legal initialization string (must start with AT). Remember not to include &W in the string! Used in fax mode.
String		FAX-INIT-STRING-2	
String		FAX-INIT-STRING-3	
String		FAX-INIT-STRING-4	
Boolean	N	MODEM-COM-1	Y or N. Despite its name, this setting no longer controls COM: ports, only which modem is activated.
Boolean	N	MODEM-COM-2	
Boolean	N	MODEM-COM-3	
Boolean	N	MODEM-COM-4	
Boolean	N	MODEM-FORCE-HANGUP	Y or N.
String	ATE1Q0V1	MODEM-INIT-STRING-1	Any legal initialization string (must start with AT). Also, remember not to include &W!
String	ATE1Q0V1	MODEM-INIT-STRING-2	
String	ATE1Q0V1	MODEM-INIT-STRING-3	
String	ATE1Q0V1	MODEM-INIT-STRING-4	
INT	1	MODEM-PORT-1	1 through 255 are legal. The COM: port to which modem-X is associated. Must be unique.
INT	2	MODEM-PORT-2	
INT	3	MODEM-PORT-3	
INT	4	MODEM-PORT-4	
INT	1	MODEM-SPEAKER-1	0 (Speaker always off) 1 (On during dialing) 2 (Speaker always on)
INT	1	MODEM-SPEAKER-2	
INT	1	MODEM-SPEAKER-3	
INT	1	MODEM-SPEAKER-4	

The **[vars]** section sets the default for per-profile variable. Defaults set in the **[vars]** section can be changed in individual profiles. **Please Note: changes in the [vars] section will only take effect for new profiles.**

Variable Name	Type	Default	Legal Variable Values
BLACKOUT-END	Time	00:00	00:00 through 23:59
BLACKOUT-START	Time	00:00	00:00 through 23:59
BUSY-REDIAL	INT	5	1 through 50
BFC-FAILED-REDIAL	INT	5	1 through 50 (How many times can a number not be bruteforced (not penetrated) before we stop dialing it)
DIAL-PREFIX	String	""	Legal phone number characters

DIAL-SUFFIX	String	""	Legal phone number characters
EFFORT-LEVEL	INT	1	1 (Connect) 2 (Identify) 3 (Penetrate)
EXPORT-ONLY-QUOTE-STRINGS	Boolean	N	Y (Only quote fields that are strings) N (Quote all exported fields)
EXPORT-VERSION-1-0-FORMAT	Boolean	N	Use the old version 1 export format (backward compatibility feature).
IMPORT-DEFAULT-TIMEPERIOD	INT	30	Default timeperiod for imported phone numbers.
FIND-MODEMS-FIRST	Boolean	Y	Y or N
MAX-CALLS-PER-NUMBER-PER-DAY	INT	-1	-1 (Unlimited) or 0 through 9999
MAX-CALLS-PER-USERNAME-PER-DAY	INT	-1	-1 (Unlimited) or 0 through 9999
MODEM-BAUD-RATE	INT	9600	300, 1200, 2400, 4800, 9600, 14400, 19200, 28000, 38400, 57600, 115200
MODEM-WAIT-TIME	INT	5	1 through 50 (sets delay in seconds between calls)
RECYCLE-NAMES	Boolean	Y	Y or N
SCAN-CARRIER	Boolean	Y	Y (Scan for modems) N (No scan for modems)
SCAN-FAX	Boolean	N	Y (Scan for faxes) N (No scan for faxes)

Appendix A: Glossary

<CR>: Carriage Return. A non-printing ASCII character meaning "Move cursor to beginning of line/end of command." Often used in conjunction with a Line Feed character, i.e. **<CRLF>.**

<LF>: Line Feed. A non-printing ASCII character meaning "move cursor to next line". Often used in conjunction with a Carriage Return character.

24-Hour Format: A way of expressing times that unambiguously designates the time of day without using the suffixes AM or PM. To express a time of day in 24-hour format, add 12 to all times after 11:59 a.m. For example, 3:00 PM becomes 15:00. Midnight is designated as 0:00. PhoneSweep uses 24-hour format to specify the time periods used to control specific dialing behavior.

911 Screening: A PhoneSweep feature that attempts to prevent accidentally calling 911 and other emergency numbers specified by the user. Sandstorm does not warrant that 911 screening will prevent all calls to emergency numbers.

Access Code: A phone number that allows access to a restricted service, such as off-site or long-distance calling. If PhoneSweep must dial an access code before or after each phone number in a profile, use the "dial prefix" or "dial suffix" options on the **Dialing** sub-tab.

Administrator: On Windows NT, the level of privilege that allows users write access to all files, to install new services, and to create new users. Analogous to *root* on a UNIX system. Because the hardware management device services must be installed, an Administrator user on Windows NT must install PhoneSweep.

Anomaly: An inconsistent response that may indicate a misconfigured or unauthorized modem. For example, a number that shifts from VOICE to CARRIER may be an intermittently available, unsecured modem. An Anomaly Detection section can be included in the PhoneSweep report.

Appendix: A section of the PhoneSweep report that lists supporting data received about calls and devices found.

Assigned Numbers: The list of phone numbers in a particular profile that PhoneSweep will call in the course of a sweep.

Bi-directional parallel port: A parallel port that can be written to as well as read from. Devices attached to a bi-directional parallel port can both receive input from the computer and return status information.

Binary bytes: Characters not printable in ASCII, sometimes included in response strings from modems. They are printed as numeric values in PhoneSweep reports.

BIOS: Basic Input/Output System. The ROM code that runs on startup and communicates with hardware to load the operating system.

Blackout period: A period of time during which PhoneSweep does not make calls. A Blackout Period can be defined without changing the time periods defined by Business Hours, Outside Hours, and Weekends.

brutecreate.exe: a utility that allows you to set the username/password combinations stored in bruteforce.txt.

bruteforce.txt: A file located in the top-level PhoneSweep directory that contains a list of username/password combinations. PhoneSweep running in Penetrate mode uses these to attempt

to log in to devices attached to remote modems it finds. The *bruteforce.txt* file can be edited or replaced with another file.

Brute-forcing: PhoneSweep's attempt to log in to remote devices it finds when scanning in Penetrate mode.

Business Hours: One of PhoneSweep's settable time periods. Defaults to 0900 (9 a.m.) to 1700 (5 p.m.). You can specify that individual phone numbers be called or not called during Business Hours.

Call History: The list of calls that PhoneSweep has made during a particular scan and the results of those calls.

Carrier signal: A tone signal that signifies a connection to a remote modem. The data exchanged by the modems is modulated in the carrier signal.

checkmodems.exe: A program in the top-level PhoneSweep directory that identifies modems and determines if they support Single Call Detect.

CID: Caller ID. A unique number in the PhoneSweep database that corresponds to a single call made, or an additional username/password guess within a call. Encountered when exporting call history.

CMOS: Complementary-symmetry Metal Oxide Semiconductors. Non-volatile memory that records BIOS settings when a machine is powered off.

COM port: another name for a serial port. Knowing which COM: ports your modems are connected to is important for configuring PhoneSweep.

Data communications: The exchange of information by two modems; communications that are not fax communications.

Data device: A device that is capable of being a modem.

Data mode: A type of telephone scan that only searches for modems.

Data modem: A modem that can only communicate with other modems and cannot send or receive faxes.

DB9: A type of serial port connector with 9 pins in a D-shaped shell. Normally used for RS-232 serial communications. Compatible with 25-pin DB-25 cabling with proper adapter connectors.

debug.bat: A file in the top-level PhoneSweep directory that performs diagnostic functions on PhoneSweep and its calling profiles.

Default button: Resets PhoneSweep to its default preference settings.

delay.exe: A program in the top-level PhoneSweep directory that allows you to schedule single and multiple sequential sweeps at specific times.

Desktop: The main Microsoft Windows window (or view).

DHCP: Dynamic Host Configuration Protocol. Allocates IP addresses to computers on request rather than each computer having a fixed IP address.

Dialing prefix: A per-profile PhoneSweep variable. Touch-Tone digits and dialing commands preceding each number to be dialed. Avoids requiring that an access code be included in each phone number. For example, a prefix consisting of the digit 9 connects to an outside line in many organizations.

Dialing suffix: A per-profile PhoneSweep variable. Touch-Tone digits and dialing commands appended to each number to be dialed. This eliminates the need to include a billing code or other suffix in each phone number.

Dialup adapter: A TCP/IP protocol stack that can be installed without requiring LAN hardware. TCP/IP is required for PhoneSweep to run properly.

DID: Direct Inward Dial.

Differential reporting: PhoneSweep function that compares the results of two telephone scans, identifying changes.

DLL file: A dynamic link library file, or shared library.

Dongle: Another term for Hardware License Management Device. When attached to a computer's parallel or USB port, allows PhoneSweep to make actual calls. The dongle prevents pirated copies of PhoneSweep from being misused.

ECP port: An Enhanced Capability Port; a type of parallel port.

Emergency Number Screening: A functionality of PhoneSweep that attempts to prevent PhoneSweep from calling 911 or other user-specified emergency numbers. See 911 screening.

Engine: The PhoneSweep task that actually places the calls. The engine interacts with the imbedded database and can be run separately from the PhoneSweep UI.

Fax device: A device capable of transmitting and receiving faxes.

Fax mode: A type of telephone scan in which PhoneSweep finds fax-capable devices but not data modems.

Find Modems First: When PhoneSweep is in Penetrate mode and this option is selected, PhoneSweep will call all numbers in the profile to locate remote modems before calling back to make brute-forcing attempts. Find Modems First is on by default.

Flash ROM: Read Only Memory that can be modified a limited number of times.

Hardware License Manager: A device that must be connected to the parallel or USB port of a computer running PhoneSweep before PhoneSweep will make any actual calls. Also called a "dongle," the hardware license manager prevents pirated copies of PhoneSweep from being used with malicious intent.

hhupd.exe: A program in the top-level PhoneSweep directory that installs HTML help on a computer that does not already have it.

I/O address: Associated with IRQs, an I/O address is internal to the computer and is used to communicate with a specific device.

Identify: At this level of effort, PhoneSweep will connect to a remote modem and then attempt to determine what sort of system the modem is attached to.

Initialization string: A command sent to a modem before each call.

IRQ: Interrupt Request. Hardware devices use IRQs to request service from the operating system when I/O operations complete or there is new data to be processed. If the operating system is not configured to know which devices are using which IRQ lines, it may crash, or the devices may be unusable.

ISA: An internal I/O bus similar to the PCI bus but older.

ISDN: Integrated Services Data Network. A digital multi-channel telephone service, more widely used in Europe than North America.

Level of effort: Specifies what actions PhoneSweep will take when it connects to a remote device. The three levels of effort are Connect, Identify, and Penetrate.

MASM: Microsoft Assembler. One of ways that non-printing characters can be represented as numbers in the report is compatible with MASM's default.

Maximum calls per day: A feature of PhoneSweep that limits the number of calls that PhoneSweep may make to a particular number in a given day.

Modem forced hangup: A process by which PhoneSweep deliberately makes an extra effort to hang up correctly after every call.

Msdun13.exe: A program in the top-level PhoneSweep directory that installs a patch for Windows95A so that the dialup network adapter's TCP/IP will function properly with PhoneSweep.

Mysqld: The SQL database server task. If it is still running after PhoneSweep exits, it must be killed before PhoneSweep can be restarted.

No Fax: Numbers listed as No Fax are those numbers which responded as "No-Fax" to a fax-mode call

Optional Sections: Portions of the PhoneSweep report that are not required under most circumstances. Can be included in the report at the user's discretion.

Outside Hours: A time period defined as weekday hours that are not covered by Business Hours. Defaults to 1700 (5 PM) to 0859 (8:59 AM) the next day. You can specify that individual phone numbers be called or not called during Outside Hours.

PBX: Private Branch Exchange.

PCI: An internal I/O bus used for add-on cards in modern desktop computers.

PCMCIA: Personal Computer Memory Card Internal Association. Also called "PC cards." A credit-card sized I/O device for laptop computers - may provide a network adapter, modem, or multiple RS-232 serial ports.

Penetrate: At this level of effort, PhoneSweep will attempt to log into devices attached to the remote modems it finds, using the username/password combinations in the *bruteforce.txt* file.

Phone number taxonomy: A listing of the phone numbers PhoneSweep has dialed in the course of a sweep, sorted by the responses PhoneSweep has elicited.

Port number: In TCP/IP, a number designating a particular service, such as file transfer, remote login, electronic mail, or PhoneSweep.

PPP: Point-to-Point Protocol. Handles Internet Protocol packets over a serial line

Profile: A list of phone numbers and associated information such as configuration settings and results of calls already completed.

Recycling: A PhoneSweep option relevant only in Penetrate mode, specifying whether PhoneSweep should try a username/password combination against one modem only or against every modem it finds in the course of a sweep.

Remote modem: A modem that answers a call made during a PhoneSweep scan.

Remote ringing: Ring tones generated by the phone switch to indicate each time a called phone line rings.

Report variable: A %STRING% in the report template that is substituted with a value when the report is generated.

Response string: The characters sent by a remote modem when it answers an incoming call, which PhoneSweep uses to identify the answering system. The full response often includes echoing back whatever data PhoneSweep sent.

Rich Text Format: A file format for text documents. It is best read in Microsoft Word, and is also compatible with WordPerfect and some other editors.

Ring timeout: A user-customizable parameter located on the **Time** sub-tab that specifies how long PhoneSweep will wait, in rings, for a response from the remote number before giving up and calling the next number. Note that ring timeout is *not* supported by most modems, including Single Call Detect capable modems. If your modem does not support remote ringing, PhoneSweep will default to using the seconds-based timeout.

Screened: Indication that a particular number was not called because PhoneSweep determined that it might connect to emergency services.

Second dial tone: A dial tone obtained by dialing an access code for services such as off-site or long distance calling. Detection of second dial tones is required in order to use PhoneSweep to detect potential toll fraud.

Sequential scanning: A mode in which PhoneSweep calls the numbers that it has been assigned to dial in ascending order. PhoneSweep's default behavior is to call the list of assigned numbers in random order. Set on the **Dialing** sub-tab.

Serial port: An I/O device that sends and receives data bytes over an RS-232 serial line. Used to connect modems and sometimes printers to PCs.

Single Call Detect (SCD): Allows PhoneSweep to evaluate calls as the connection sequence takes place and modify its behavior accordingly. SCD allows fast, accurate voice recognition and decreases the total number of calls that need to be made in the course of a sweep by avoiding unnecessary second calls to data devices while looking for fax-capable devices.

Sleep Mode: A power-saving mode implemented by some desktop and laptop computers. If disk and communications activity only will not prevent the computer from entering sleep mode, then sleep mode must be disabled before leaving a PhoneSweep scan running unattended.

SQL: Structured Query Language - A standard language for database access. PhoneSweep uses an SQL database to store data.

Sub-tab: A tab in a row that appears on the left side of the PhoneSweep window when the options **Setup tab** is clicked. The options on the sub-tabs set the configuration for the current profile.

Sweeping: The process of methodically calling phone numbers, taking the actions specified in the level of effort, and recording the results of the calls. Also referred to as Telephone Scanning.

Tab: An area on the PhoneSweep UI that can be selected to reveal a set of related information or configuration options.

TCP/IP: The major networking protocol of the Internet. PhoneSweep uses TCP/IP to communicate internally among the engine, database and UI.

Telephone Extender: A number or extension that is dialed to allow access to long-distance services or tie lines.

Telephone line scanner: The term Sandstorm has coined for dialing software specifically designed for use as a security auditing tool.

Testing injury: An undesired result of running PhoneSweep, such as accidentally calling emergency services. The PhoneSweep license agreement explicitly states that the end user assumes all liability for any testing injuries

Time Period code: A value associated with each phone number that specifies during what time periods the number may be called. When importing numbers from a file, a default value of 30 (call during any time period) is applied to any numbers that are read without a valid time period.

Timeout: The number of seconds that PhoneSweep will wait for a response from a remote number before it gives up and goes on to the next number. Used with modems that do not support remote ringing. Set on the **Time** sub-tab; default values are 50 seconds in Business Hours, 92 seconds otherwise

Unknown: All phone numbers have a default status of Unknown System when a profile is created. This status only changes on Carrier lines in Identify and Penetrate Levels of Effort where PhoneSweep is able to identify the system.

Unprintable characters: Characters that cannot be represented as ASCII characters. Unprintable characters sent in modem response strings can be printed as numeric values in the report. The maximum number of non-ASCII characters that will be printed in a single line can be set on the **Report** sub-tab.

Unsecured modem: A modem connected to a system that allows login without a password or with an easily guessed password.

USB interface: Universal Serial Bus. A serial I/O channel to which multiple peripherals can be connected, most commonly found in laptops.

Username/password recycling: An option settable on the **Effort** sub-tab. When **Recycle Names** is set in Penetrate mode, each username/password combination in *bruteforce.txt* will be tried against each modem found.

Weekends: One of the three time periods during which PhoneSweep's dialing behavior can be defined; defaults to 0:00 to 24:00 Saturday and Sunday. Time periods can be set on the **Time** sub-tab.

WinSock: A Windows TCP/IP implementation; a library that provides networking services for applications.

W95ws2setup.exe: A program in the top-level PhoneSweep directory that installs the WinSock 2.0 API on your computer.

Appendix B: PhoneSweep FAQ

The PhoneSweep FAQ is a collection of Frequently Asked Questions and answers about normal PhoneSweep operations. For information on diagnosing problems and troubleshooting, please see Appendix C: PhoneSweep Troubleshooting Guide.

This FAQ is arranged by topic. If a specific question and answer belongs in two categories, it will appear in both.

Single Call Detect (SCD)

Why does SCD make two calls to some numbers?

The "single" in Single Call Detect refers to the fact that PhoneSweep with SCD adapts its dialing behavior to avoid unnecessary second calls to extensions that do not reach modems or fax machines. It schedules second calls only to devices that may be capable of both fax and data communications. Conventional telephone scanners must make two calls to all numbers, one in data mode and one in fax mode, to find fax-capable devices. In SCD mode, PhoneSweep avoids this duplication.

How do I know if my modem supports SCD?

Running *checkmodems.exe*, a program in the top-level PhoneSweep directory, will tell you if your modems support SCD. You can also check Sandstorm's list of SCD-capable modems at http://www.sandstorm.net/support/phonesweep/reccmodems.shtml.

Can I scan for only data (Modem) or only fax devices in SCD mode?

Yes (this became a feature as of PhoneSweep 2.01).

Will PhoneSweep running in SCD mode find an answering machine/fax combo?

No. PhoneSweep will only detect answering machine/fax devices during scans in Fax-only mode. SCD will report them as Voice. If you need to find answering machine/fax combinations, run two scans, one scanning for both Fax and Modems and the second scanning for just Fax machines, then make a Differential Report comparing the results of the two scanned profiles. Phone Numbers that come up first as Voice in the first scan, and as Fax in the second scan will be reported as anomalies. (Please see below, under "Using PhoneSweep" and Detecting Line Sharing devices for additional information.)

Using PhoneSweep

Can I use phone numbers from any country? Do they have to be a certain length?

You can use phone numbers of any length for any country. In some instances it makes sense to place common beginnings and endings within the **Prefix** or **Suffix** (Such as when you need to dial 8 or 9 to get out of a Phone System).

Why do I need to Force Modem To Hangup?

If a modem doesn't hang up properly after a call, further calls will fail because there won't be any dial tone. This option is usually not needed, but may help if modems don't hang up properly after a call. Enabling **Force Modems To Hangup** will slightly increase the time taken by each call. Devices running programs such as PC Anywhere often don't release the phone lines promptly.

Can I use a profile created by one version of PhoneSweep with another version of PhoneSweep?

Normally, yes. When it is necessary to revise PhoneSweep's database structure, we can ensure that newer versions of PhoneSweep will read (and convert) older profiles, but we cannot make older versions read newer profiles. For this reason, profiles created with PhoneSweep version 1.03 or later cannot be used by PhoneSweep version 1.02 or earlier. Profiles created in PhoneSweep 3.0 and later can be used by PhoneSweep 2.04, but you will not be able to access associated notes.

Can PhoneSweep dial sequentially through multiple profiles without human intervention?

Not directly. If you can estimate how long it should take to dial each profile to completion, you can use *delay.exe* to make PhoneSweep begin dialing a second profile after the first one finishes. Contact Sandstorm for further information.

Why is PhoneSweep ignoring the ring timeout and using the seconds-based timeout?

Most modems, including SCD-capable modems, do not support remote ringing. If the modem does not support remote ringing, PhoneSweep will use a seconds-based timeout. This can be adjusted to equal the desired ring timeout.

How does PhoneSweep deal with numbers that it first records as busy?

They are called back multiple times. The Busy Redial field on the **Dialing** sub-tab controls the number of times. The default value is 5 re-tries.

Can I select only the numbers in a profile that are reported as BUSY and call them back at a later time?

Starting with PhoneSweep 3.0, you can export all BUSY numbers into a text file, which can be imported into another PhoneSweep profile and swept as usual.

Why does PhoneSweep default to calling numbers in the profile in random order?

This avoids problems with systems that limit repeated calls. Successive callbacks to sequential numbers might also irritate users.

What is the difference between "Timeout" and "Ring Timeout"?

Ring Timeout is a more specific instance of Timeout. "Timeout" means that no connection was made. This can mean that the number was never answered (ring-based timeout), or that a person answered but their voice was not detected, or that the line was picked up but no sounds or tones came from the other end (seconds-based timeout). SCD will reduce the incidence of the last two cases, because if the line was picked up, SCD defaults to VOICE. Ring Timeout means the call was dropped after waiting the maximum number of rings allowed.

How can I delay a scan?

Use the **Schedule Start and Stop** commands under **Start** in the **File** menu to control when calling begins, or change the Time Periods to control when calling actually begins.

Can I get PhoneSweep to add a range of numbers except for a few numbers?

No, but you can add a range and then delete the non-desired numbers. Alternatively, you can use a database or text-processing application to build the range and then make the selective deletes, and import the file into PhoneSweep.

Do the modem drivers need to be installed for PhoneSweep to work?

No. PhoneSweep uses the low-level COM port drivers instead of TAPI.

Will HTML Help run if the computer running PhoneSweep does not have Internet Explorer installed?

Probably yes, if you run *hhupd.exe* in the top level PhoneSweep directory. Note, however, that having IE installed on a computer does not mean that you have to use IE at all; you can keep running your preferred web browser.

Can I use PhoneSweep with Remote Software?

We have performed some testing with PhoneSweep with PCAnywhere and NetOp, but we cannot guarantee 100% compatibility. Make sure such software loads and operates correctly on its own before you attempt to use PhoneSweep over it.

Can PhoneSweep dial through an automated teller?

Not always. To find out if you can, place the main phone number in the **Prefix** field on the **Setup->Dialing sub** tab. Then add the extensions or internal lines to the profile, either through the **Phone Number** tab or **Import** button.

It is important that you be aware how many seconds pass from when the main system picks up, and when it can take the extension numbers. If need be you can add commas to the end of the **Prefix** to make PhoneSweep pause until the answering system is able to take phone numbers. Each comma usually causes a pause of 1 second. You can change this value by adding S8=N, where N = a value in seconds, to the init string for each modem.

If each number needs a code, you need to make that code part of the phone number (Import using double quotes around code and phone number together: "code,Phonenumber" or "Phonenumber,code").

Please call Sandstorm Support for further details when setting this up.

Can PhoneSweep detect Line-Sharing Devices?

Depends on how the Line-Sharing devices are set up. If no code is needed, then you may need to scan twice, first looking for fax machines only, then looking for modems only, in order to find attached devices. If a line defaults to voice and you scan for both faxes and modems, then the line will come up as voice.

If a code is needed to access devices or Voice, then you would need to use supply the profile with a separate instance of the phone number with a code for each device or voice on the shared line (you may need to use a comma between the phone number and access code). We suggest you use a note for each number as well, so you can quickly scan information. On the Profiles you would see:

555-1000,3 note: fax code =3

555-1000,4 note: voice code =4

Can PhoneSweep detect Dial-back modems?

Possibly as a System if the dial-back system uses ASCII text, otherwise, no. At best PhoneSweep may identify a dial-back line as "Tone".

Can PhoneSweep detect Reverse Carrier Tone modems?

Before PhoneSweep can detect a Reverse Carrier Tone modem you need to set your modem initialization strings to detect reverse tones and set PhoneSweep to "Never use Single Call Detect".

During normal PhoneSweep operations, Reverse Carrier Tone modems should be identified as "TONE", using the default init strings and "Use Single Call Detect if available….". If you encounter such modems, please contact PhoneSweep Technical Support with the modem make and model.

Please remember to remove the Reverse Tone command from your modem init strings after scanning.

Can I use PhoneSweep with Gold pack add-ons?

Yes, with PhoneSweep 4.0 and above.

What are the Gold add on capabilities and how are they useful to me?

Gold add-on options extend PhoneSweep's standard capabilities:

- Distributed (2 copies PhoneSweep, each with Gold add on required) allows you to remotely administrate distant copies of PhoneSweep via a local copy of PhoneSweep.
- E-mail notifications allows you to set automatic e-mail notifications when PhoneSweep encounters the events you specify.
- Merged Reporting allows you to generate a single report from multiple profiles, each with different phone numbers.

Improving PhoneSweep's Performance

How can I get PhoneSweep to make more calls per unit time?

Reducing the level of effort will allow PhoneSweep to progress through the profile more quickly. Some suggestions include:

- Complete the scan at a low level of effort, and then rescan only the numbers that gave anomalous results at a higher level of effort.
- Use a modem that supports Single Call Detect (SCD).
- Reduce the values of **Single Call Voice Timeout** and the timeouts on the **Time** sub-tab; however, this will make PhoneSweep more likely to miss modems that do not pick up quickly.
- Decrease the **Busy Redial** count.
- Decrease **Delay Between Calls,** but it is not recommended to decrease it below 5 seconds. Doing so may not allow your modem enough time to reset itself between calls, and can generate mis-identifications.

In general, configurations that make the scan go more quickly risk losing information and accuracy, except in the case of enabling SCD. It's a tradeoff; decide how much detail and accuracy you need in your report.

Can I use a multi-modem version of PhoneSweep to simultaneously dial multiple profiles?

No. PhoneSweep Plus and Plus-8 will make more calls per unit time and therefore take less time to finish scanning a profile, but only one profile can be active at a time. PhoneSweep Plus 12 and Plus 16 will still dial faster.

Can I set PhoneSweep to sequentially dial through multiple profiles without human intervention?

Not explicitly, but you can use a workaround with the *delay.exe* command once you create the profiles, if you can estimate how long it will take to scan each profile. (Contact Sandstorm for more information on *delay.exe*.)

Would dialing into an organization from outside the organization's PBX rather than using PhoneSweep internally impact PhoneSweep's performance?

One disadvantage to conducting a PhoneSweep security audit from outside the organization's PBX is long-distance charges, but only if they apply to the calls you need to make. Dialing an organization's phones from within its PBX can be slightly faster due to fewer digits being dialed and shorter call set-up times. The speed increase is rarely more than 10 to 20%.

Sometimes dialing from inside a switch can cause problems with Single Call Detect. Typically the result is obvious, such as half of all calls being identified as TONE.

Fax machines and Fax/Modems

What is a fax/modem? What kind of a security risk do they pose?

A fax/modem is a device that is capable of both fax and data communications. For security purposes, a fax/modem is at least as dangerous as a data-only modem, and is probably more dangerous than a normal modem. The user who installed the fax/modem may believe that it is answering only fax calls and be unaware that it can also auto-answer data calls, and thus may not take any steps to secure the machine.

Do fax machines pose a security risk?

Yes. A user who has authorization for an analog line for fax machine use can intentionally use the analog line to provide a data connection.

How would a fax/modem be reported if PhoneSweep were set to scan for only data or only fax?

A fax/modem will be reported as Fax by PhoneSweep running in fax-only mode and Carrier in data-only mode.

Why is a number first reported as Fax and subsequently reported as Carrier?

That number reaches a fax/modem; fax detection takes place first with SCD.

When might PhoneSweep miss a fax machine?

If PhoneSweep reaches a fax machine that makes non-fax tones or plays a prerecorded message when it answers the call (as in the case of an answering machine/fax combination and some **Super Group 3** fax devices), PhoneSweep will record the call as something other than Fax. Another possibility is problems with your phone switch that make PhoneSweep thinks that the call has been answered when it hasn't been, or forgetting a dialing prefix. Most misidentifications occur at the Connect level of effort, where PhoneSweep only listens to tones and hangs up.

The **Super Group 3** protocol is the marketing term for faxes that push the Group 3 fax protocol to its upper limits when transmitting fax signals at 36.6 K using compression.

Finding All the Modems

How do users attempt to hide unauthorized modems?

Users who do not want their unauthorized modems to be caught by a PhoneSweep scan may turn them off when the modems are not in use, configure the modem for dial-out only, or configure the modem such that it only picks up after a large number of rings. Fortunately, these measures also make the modems harder for attackers to find.

How can I increase my chances of detecting rogue modems that the user has attempted to hide?

To catch rogue modems that are only turned on part of the day, enable the **Dial During Each Time Period** option when adding phone numbers to the profile. To find modems that have been set to pick up after an abnormally long number of rings, increase the **Timeout** or **Ring Timeout** as appropriate on the **Dialing** sub-tab.

How do I make sure unauthorized modems have been removed?

Do another sweep on the same numbers with the **Rescan** button.

What if voice mail picks up first on a line that has an unauthorized modem on it?

If voicemail always picks up before the modem, the modem is not vulnerable to attack. If you are concerned that voicemail is only picking up part of the time, you can schedule calls to that particular number during different parts of the day by specifying Dial During Each Time Period when adding these numbers to the profile.

Will a remote modem configured for dial-out only be classified as Timeout?

Yes.

When won't PhoneSweep attempt to Bruteforce (Penetrate) a System?

PhoneSweep will not attempt to Bruteforce Callback systems that accept ASCII text, nor will it attempt to bruteforce unknown systems that do not have recognized username or password request. If you feel that PhoneSweep should be able to penetrate a given system, please generate a Report with **Appendix A** and then contact Sandstorm Technical Support.

Evaluating Security Risks

How is toll fraud committed? How can PhoneSweep help me detect toll fraud?

Unethical persons can dial into an organization's PBX and use internal toll-access numbers to make long-distance calls that are billed to the organization. PhoneSweep helps you guard against this situation by detecting second dial tones.

Do second dial tones pose any security threat?

Yes. An unexpected second dial tone may be vulnerable to toll fraud, if it can be accessed from outside the organization.

Other than actual lines in use, what might Busy numbers indicate?

A busy phone number may be an incorrectly configured line that gives a fast busy tone. If all numbers in a profile are reported as busy, PhoneSweep may be having a problem dialing out. See Appendix C: PhoneSweep Troubleshooting Guide.

Do fax machines pose a security risk?

Yes. A person allocated a line for a personal fax machine may decide to attach a modem to it, without asking for authorization or properly securing the machine.

Do fax/modems pose a security risk?

Yes. It is possible that a fax/modem may pose more of a risk than a data-only modem. Users may not realize the necessity of securing a fax/modem.

What should I do about numbers that always time out?

Your response to numbers that consistently time out depends on your threat model. Typically, you should check to see if the line is actually connected to anything. A number that always times out could be a modem that does not pick up for a large number of rings, but this is uncommon and is not likely to be a major security risk.

The PhoneSweep Report

Why is special handling of unprintable characters in Appendix A of the report necessary?

Unprintable characters cannot be represented in ASCII. On the **Report** sub-tab you can adjust the number of non-ASCII characters that will be printed as numeric values on a single line. If this limit is exceeded, PhoneSweep reports the number of characters not printed.

When a modem becomes disabled during a sweep, where are the errors recorded?

phonesweep.log in the top-level PhoneSweep directory.

Ethical Considerations

Can I get in trouble for using PhoneSweep?

Yes, if you use it without proper authorization, or in a manner that disrupts business or violates laws. It's your responsibility to understand the relevant local laws and your organization's policies.

How do I know that PhoneSweep will not hang systems that it calls? I'm concerned about PhoneSweep disrupting business or services being offline to customers.

The first step is to conduct scans at times when services are not in heavy use, for example at night. Divide your first scan into per-night scans. Also, before you begin production scanning, do a test scan on non-critical systems to ascertain how your environment interacts with PhoneSweep.

PhoneSweep has timeouts that cause it to disconnect from a remote number after a specified amount of time has passed. If remote software is not properly configured, calling that number without the proper protocol can result in the system crashing or leaving the phone off-hook for several minutes. While there is potential for disruption, note that remote software configured in this way is a serious Denial Of Service vulnerability and should be corrected.

Miscellaneous Questions

What are the advantages of the SQL database?

The SQL database is flexible. It allows for easier updates and a wide range of possible import/export formats. It also allows users to build customized reports using criteria more specialized than those in the PhoneSweep report and the export options.

Will an RTF PhoneSweep report fit on a floppy?

The answer depends on the options selected and the number of calls in the profile. Note that if the report is too large in normal RTF format, most data file compression tools will reduce the size significantly.

When I start a sweep, does Phone Sweep start dialing? For example, when I start a sweep at 5pm and my outside business hours start at 7pm: will PhoneSweep dial any numbers between 5pm and 7pm?

Only if there are phone numbers that have been assigned to be swept during business hours. When PhoneSweep starts dialing, PhoneSweep checks the current time period against the time periods set for the phone numbers in the current open Profile. If no phone numbers are set for the current time period, then PhoneSweep will not dial any numbers.

Appendix C: PhoneSweep Troubleshooting Guide

This section contains information that can help resolve problems that crop up in the course of running PhoneSweep**. Please read this section before contacting Sandstorm Technical Support.** Many problems have uncomplicated solutions, and this section will usually give the quickest way to get PhoneSweep up and running again.

This section is divided up into several subsections:

- Information you should have available while troubleshooting PhoneSweep.
- Easily rectifiable situations that may cause problems running PhoneSweep.
- Common problems encountered while running PhoneSweep and possible solutions for them.
- Error messages, their causes and possible solutions.
- The *debug.bat* file and debugging information for advanced users.
- Other things to try.

Information To Collect Before Troubleshooting

- **Error Messages**: Make a note of any error messages, *including their exact text.* Error messages may appear in dialog boxes and can also be viewed in the file *phonesweep.err*. Error messages may also appear on the **History** or the **Status** tabs.
- **Operating System**: What version of Windows is PhoneSweep being used with? Some problems are OS-specific.
- **Modem**: What brand and model of modem was PhoneSweep using to dial? What does *checkmodems.exe* say about your modem? Many problems can result from using a misconfigured or non-recommended modem, because PhoneSweep's performance depends heavily on the modem. **If *checkmodems.exe* can find your modems, but PhoneSweep cannot, have you set the correct COM port for your modem in PhoneSweep?**
- **PBX**: What make/model PBX do you use? How does your PBX handle voice mail messages when callers hang up? Does it leave a beep when callers hang up?
- **Phone System**: What make/model phone system are you using? How is it configured to handle voice mail?
- **Version number**: What version of PhoneSweep was having problems? Often, bugs found in older versions of PhoneSweep will have been corrected in subsequent releases.
- **Level of Effort**: Make a note of the level of effort PhoneSweep was using when the problem occurred.
- **Scanning mode**: What kind of devices was PhoneSweep scanning for when the problem occurred? Was PhoneSweep running in Single Call Detect mode? Were you scanning for just modems? Just faxes? Faxes and modems?
- **Patterns**: Is there a pattern to the type of calls that cause problems? For example, does the problem occur only when calling internal extensions?

- **What changed since things last worked**? When PhoneSweep "just stops working," the reason is usually a side effect of some other change to the computer or its environment. Check your modem cables, telephone jacks and the software environment (O/S changes, new applications using the COM port, internal security software, etc.). Also, ask your telecommunications service if they have performed any work on the phone system that might have affected PhoneSweep.

Things To Check If You're Having Trouble

- **Are you running PhoneSweep with a non-recommended modem**? The quality of the information collected by PhoneSweep depends heavily on the modem used to place the calls. Try sweeping with a recommended modem. The updated list is at http://www.sandstorm.net/support/phonesweep/reccmodems.shtml.
- **Was a screensaver or other software (such as a virus checker) running simultaneously with PhoneSweep?** Try disabling the screensaver or other software and restarting PhoneSweep. If this does not work, disable all non-essential software before restarting PhoneSweep. If this is the problem, and you need to lock your screen, we recommend the third party product, ScreenLock, which can be run on Win '95, '98, NT 4.0 and 2000. You can obtain it from http://www.screenlock.com.
- **Is the hardware license manager attached to the parallel or USB port and firmly seated?** PhoneSweep cannot make any calls unless the license manager is in place. If the license manager disengages from the parallel or USB port while PhoneSweep is running, PhoneSweep will stop dialing. Reattach the license manager and restart PhoneSweep. If you are using Windows NT, you may need to re-boot your PC.
- **Are you running PhoneSweep on a laptop running on battery power?** The laptop may not automatically activate the port that the dongle is plugged into. If you can't plug in the laptop, attach a device with an independent power supply, such as a printer or fax machine, to the dongle and restart PhoneSweep.
- **Are you running PhoneSweep on a laptop with Windows NT?** PhoneSweep works best on laptops that are running Windows 95/98. If you have the option of running PhoneSweep under one of these operating systems, do so.
- **If you are running PhoneSweep under Windows NT, 2000 or XP, was the dongle attached to the parallel or USB port and firmly seated during installation?** The dongle must be attached during the Windows NT install for PhoneSweep to install correctly. If the hardware license manager was not attached to the correct port during the PhoneSweep installation, attach the hardware license manager to the correct port and follow the directions in Section 3.6, **Hardware License Protection**, to reinstall PhoneSweep.
- **If you are running PhoneSweep under Windows NT, 2000 or XP, were you logged in as an Administrator when PhoneSweep was installed?** To run correctly under Windows NT, 2000 or XP, an Administrator must install PhoneSweep.

- **If you are running PhoneSweep on Windows NT, 2000 or XP, do you have write permission for the PhoneSweep directory?** If you want to run PhoneSweep as a non-administrator, PhoneSweep must be able to write to its log and profile directories. An administrator can reset the Security values under the Properties of the PhoneSweep directory.

  If you are running PhoneSweep under certain system configurations or security settings, it is possible that PhoneSweep may need to be run by an Administrator. Doing so will guarantee PhoneSweep access to the files, devices and system services it requires.

- **Did you copy missing DLL files from another computer?** Copying DLL files from one computer to another does not work. If you are running PhoneSweep on a Windows NT system and you get an error message stating that you are missing DLL files, try installing Internet Explorer 4.01 or higher, and upgrading to a newer NT service pack.

- **Are you running Windows 95A?** There is a bug in Windows95A that prevents PhoneSweep from running correctly. This is not an issue with Window 98 or Windows NT. If clicking in the My Computer icon on a Windows 95 machine does not indicate under "system" that you are running a version ending in the letter B, run the program *msdun13.exe* in the top-level PhoneSweep directory to correct the problem, then restart PhoneSweep.

- **Do you already have another copy of the PhoneSweep engine or database running?** Hit CTRL-ALT-DEL to bring up the Task Manager and kill any processes named PhoneSweep or MySQLd and restart PhoneSweep.

- **Are you using a dialup adapter for network connectivity?** If your computer is configured such that the dialup adapter TCP/IP protocol stack is only loaded under certain circumstances (possibly when under DHCP), PhoneSweep will malfunction. For more information about the dialup adapter, see the section on PhoneSweep installation.

- **Does the computer on which you are running PhoneSweep meet the system requirements?** See Section 3, **Installation and Setup**.

- **Is any other software running simultaneously with PhoneSweep?** In rare instances, some software may conflict with PhoneSweep, most often when attempting to share COM ports. Try shutting down all other programs and restarting PhoneSweep. It has also been reported that having Norton Autoprotect installed on a computer can cause a general protection fault when the PhoneSweep InstallShield installer is running.

- **Are there incoming calls on the line PhoneSweep is using to dial out?** If so, PhoneSweep may inadvertently answer them and report modem errors. This should be avoided by changing phone lines if necessary.

Common Problems and Possible Solutions

- **PhoneSweep will not start sweeping**. If you click on Start and PhoneSweep does not begin sweeping, first collect some information and refer to the more specific situations below. Make sure the dongle is attached and firmly seated, the modems are turned on, at least one modem is selected on the **Modems** sub-tab, the COM ports do not have any IRQ conflicts, and that you are not in a time period when PhoneSweep is not allowed to make calls.

- **PhoneSweep starts up, but does not begin placing calls**. It is possible that you are in a time period or a blackout period during which PhoneSweep is not allowed to make any calls. Check the icons along the bottom of the PhoneSweep window. Also, if PhoneSweep is started without the hardware license manager firmly attached to the parallel or USB port, PhoneSweep will run

only in demonstration mode and will not place any actual calls. Attach the hardware license manager to the parallel or USB port and restart PhoneSweep.

- **When the sweep is started, PhoneSweep immediately reports that it is finished and stops the sweep**. PhoneSweep may think that it is not allowed to dial any of the numbers during any time period. This may be because the definitions of the time periods have been changed, or because Blackout Hours have been set incorrectly. Compare the **Phone Numbers** tab with the **Time** sub-tab, and review the documentation on time periods and importing data.
- **PhoneSweep starts sweeping, but the modems do not begin dialing.** Check to see that the hardware license management device is attached to the parallel or USB port and firmly seated. PhoneSweep will only run in demonstration mode and not make any actual calls if the hardware license manager is disconnected. This can be also be caused by a defective modem, loose cables, or not having selected any modems in the **Modems** sub-tab.
- **PhoneSweep stops dialing during a sweep.**
  - Check to see if the hardware license management device has become loose or disconnected from the computer's parallel or USB port.
  - Check the **Time** sub-tab to be sure that you have not entered a period during which PhoneSweep is not allowed to make calls.
  - If you have PhoneSweep set to dial in **Sequential** mode (set on the **Dialing** sub-tab) and have limited the number of calls that PhoneSweep is allowed to make per number or username per day, PhoneSweep can get into a state where it is not allowed to make any further calls. Try disabling sequential mode.
  - Enable **Force Modems To Hangup** on the **Dialing** sub-tab. If a modem fails to hang up properly, it will not get another dial tone and will be unable to make further calls. If you are using a multi-modem version of PhoneSweep and the modems stop dialing one by one, it is likely that your modems are not hanging up properly.
  - Do you have incoming voicemail on the line the modems are dialing out on? If so, the "stutter" of the voicemail notification may cause your modem to disconnect without getting a dial tone. Try increasing the S6 setting in the **Init String** field on the **Modems** sub-tab.
  - Is a prerecorded message playing after each call you make hangs up? If so, PhoneSweep may not wait long enough to get the next dial tone and therefore stop dialing. Try increasing your S6 setting in the **Init String** on the **Modems** sub-tab so PhoneSweep waits long enough to get a dial tone.
  - If you are dialing in Single Call Detect mode, try sweeping with Single Call Detect disabled (**Dialing** sub-tab).
  - Do you have other software running on the computer? Try disabling all other software before running PhoneSweep. Contact Sandstorm if this does not work.
  - Did anyone call your PhoneSweep modem lines during the sweep, or is anyone sharing your line? (rare)

- **The PhoneSweep UI freezes during a sweep**. If you encounter this symptom, please contact Sandstorm.
- **PhoneSweep stops dialing in the middle of a sweep when no one is around to restart the sweep**. To re-enable all disabled modems and cause PhoneSweep to restart dialing, use the Delay command to automatically restart the sweep a few hours in. This is a stopgap solution; please see the entries under "PhoneSweep stops dialing during a sweep" above to diagnose the cause.
- **PhoneSweep hangs when it calls one particular number**. If you encounter the problem, put the problem number in a profile by itself. This lets you complete the original profile without the problematic number. Next, please contact Sandstorm Enterprises so we can work with you to isolate the cause.
- **PhoneSweep is leaving blank voicemail messages**. First, try enabling Single Call Detect. If PhoneSweep running in Single Call Detect mode with a recommended modem still leaves blank voicemail messages, try setting **Single Call Voice Timeout** in the **Dialing** sub-tab to a lower value, for example 3 or 4 seconds (this can also be set via the variable SINGLE-CALL-VOICE-TIMEOUT in the *phonesweep.ini* file). Note, however, that setting this variable to a lower value may increase the chances that some modems may be missed during the sweep.

  When PhoneSweep is scanning in fax mode, it leaves a message containing fax tones on voicemail. Try enabling Single Call Detect by selecting the appropriate option on the **Dialing** sub-tab.
- **PhoneSweep is progressing through the profile too slowly**. First, determine what would be a reasonable number of calls per hour for PhoneSweep running under the particular conditions. PhoneSweep running in Penetrate or Identify modes will take longer to progress through a profile than it would in Connect mode. Therefore, if you do not need the level of information gathered in Penetrate or Identify mode, consider reducing the level of effort. Also, enabling username/password recycling when scanning in Penetrate mode increases the amount of time necessary to finish a profile. Enabling Single Call Detect will reduce the amount of time needed to complete the scan, as will turning down the timeouts. Reducing timeouts may cause PhoneSweep to miss modems.
- **PhoneSweep inaccurately identifies devices**. The quality of the information gathered by PhoneSweep is highly dependent on the quality of the modems used to dial. Try using a modem that Sandstorm recommends as working well with PhoneSweep. PhoneSweep cannot identify some exotic devices such as encrypted telephones. Check to see if your phone switch is making odd noises or if you're forgetting a dialing prefix.

  In some cases, PhoneSweep may interpret voicemail tones as fax tones. Also, sometimes when dialing out through a switch, the switch makes a click or tone as it hands off the call, causing PhoneSweep to believe that the call has already been answered. Try calling the misidentified numbers in a way other than dialing through the phone switch.

  If the misidentifications are related to dialing internal versus external extensions, it is possible that your phone switch is making a tone when it calls an internal or an external extension, or there may be a different type of ring when calling internal versus external extensions. Calling the misidentified numbers and some correctly identified numbers with the modem speaker enabled can be instructive.
- **Fax machines are reported immediately as BUSY**. It is possible that PhoneSweep is not waiting long enough between calls. Increase the Delay Between Calls parameter on the **Time** sub-tab.

- **PhoneSweep identifies all numbers as a busy signal**. This indicates a possible problem with dialing out. PhoneSweep may be missing a dial tone or a connection to an outside line. If you need to dial a prefix to reach outside lines and need to dial this prefix for each number in your profile, enter the prefix in the appropriate field on the **Dialing** sub-tab. Increasing the delay between calls on the **Time** sub-tab may help if the problem is not a missing prefix.

  This may also be a problem with using modems programmed for American phone systems in European countries whose dial tones sound like American busy signals.

- **PhoneSweep identifies all extensions as second dial tones**. This may occur if PhoneSweep is dialing internal lines when it has been configured to always dial an access code for an external number before each phone number. If a prefix has been specified on the **Dialing** sub-tab or in the *phonesweep.ini* file, remove it. Also, try placing PhoneSweep outside the PBX, or disabling **Single Call Detect**.

- **PhoneSweep gives a call result other than CARRIER on a number known to have a modem on it**. The modem may not be set to auto-answer, in which case a VOICE response will occur if your PBX system is set to forward the call to voicemail, or a TIMEOUT response if the phone does not pick up. Also check to be sure that the number isn't being used by a PhoneSweep modem, in which case you would either get a BUSY or a VOICE response.

  Important Tip: If a number is giving unexpected results with PhoneSweep, use your phone and call the number yourself. This may help you identify the problem.

- **PhoneSweep running in Identify or Penetrate mode fails to identify systems**. It is possible that PhoneSweep does not have the unidentified system(s) in its database. Contact Sandstorm Enterprises with the response string from the unidentified system and we will add the system to PhoneSweep's database.

- **A device was penetrated while PhoneSweep was running in Identify mode**. This usually means that PhoneSweep logged directly into the system with no username or password authentication needed. This is a major security vulnerability.

- **HTML help doesn't work**. Try running the HTML help installer *hhupd.exe* in the top-level PhoneSweep directory. If this doesn't work, try installing Internet Explorer 4.01 or 5.0 on your computer or, on an NT system, upgrading to a newer service pack.

- **PhoneSweep reports that a DLL file is missing**. Copying DLL files from one computer to another does not work. Installing Internet Explorer 4.01 or higher and reinstalling PhoneSweep may clear up the problem. Upgrading the service packs may help; there may be a way to get DLL files from the NT service packs.

- **PhoneSweep stops working after an NT workstation upgrade**. This is likely a Microsoft problem; installing Internet Explorer 5.0 may clear up the problem.

- **PhoneSweep is not making brute-force attempts when set to Penetrate mode**. PhoneSweep can only brute-force systems that it can at least partially identify.

- **PhoneSweep is using the seconds-based timeout instead of the ring timeout.** Most modems, including those that support Single Call Detect, do not report remote ringing. Adjust the seconds-based timeout on the Time sub-tab to coincide with the proper number of rings.

- **Running a screensaver makes PhoneSweep lock up**. Unfortunately, there is currently no way to ensure that PhoneSweep will run correctly if a screensaver is running at the same time. There is no way to predict whether PhoneSweep will or will not have problems with a given screensaver. Disable the screensaver if it appears to be causing problems. We have tested a third party product called Screen Lock. It works on Windows 95/98/NT/2000 and allows you to run PhoneSweep and other programs in the background. You can obtain it from http://www.screenlock.com.
- **I cannot get a multi-port serial card to work.** Resetting the cards and connections is a good place to start. If you have multiple cards, try swapping them, and/or swapping their cables. If nothing else works, uninstall the cards and drivers and start over.
- **I've reseated the multi-port serial card or its cable several times, and I still can't get my computer to acknowledge the card.** It is possible that the card and/or cable are defective. If possible, try to install the card on another machine, preferably one with different hardware or operating system. If you are able to install the card on another machine, have your company's technical support personnel check your own machine's settings. After testing, if it appears that the card and/or cable are defective, call the manufacturer. If you bought the card from Sandstorm, please call our Technical Support department.
- **I installed a multi-port serial card, but I cannot set my UART's or COM ports for modems.** Some machines (especially Dell Optiplexes) are picky about where you place multi-port cards. If you are using a SeaLevel card on a Dell Optiplex, try moving it to the middle port. On other machines, move the card to the port normally used by the internal modem (this usually maps to COM 2 or 3).
- **I added a multiport serial card, but fewer COM ports are visible in software than I expected**. Remove the card and reboot the computer, and see if the number of COM ports increases. If not, you may have a resource conflict. Try re-installing the hardware and drivers.
- **I am using an 8-modem card, but only COM ports 5-10 are found**. On some systems, you may need to manually install the modem drivers on COM ports 11 and 12).
- ***checkmodems.exe* is not identifying the devices on the COM ports correctly**. Check the settings in the Device Manager and ensure that they are correct. If this is not the problem, try one of the following:
  - Turn the modem(s) on and off; reseat all connections involved.
  - Swap modems and cables (and multi-port serial cards if you are using them) to see if the problem is associated with a particular piece of hardware.

  If the problem follows a particular piece of hardware, or you cannot fix it, contact the manufacturer or Sandstorm Technical Support if you purchased your modems from us.
- ***checkmodems.exe* hangs at one port.** Try resetting the modem at that port, and reseating its cable. Try swapping cards and/or cables if you are using a multi-port serial card.
- **PhoneSweep isn't running in Single Call Detect (SCD) mode**. Run *checkmodems.exe* to make sure that your particular modem supports SCD. Modem manufacturers may change the chipset of a particular model of modem without warning or documentation. Make sure that you have specified SCD mode on the **Dialing** sub-tab as "Use Single Call Detect if available, regular dialing if not." Also, be sure that you are dialing for both carriers and fax machines.
- **PhoneSweep running in SCD mode makes two calls to some phone numbers**. This is probably normal behavior. PhoneSweep in SCD mode schedules second calls to only those

devices that it determines are capable of fax communications. If SCD is making two calls to all numbers, use *checkmodems.exe* to make sure that your particular modem supports SCD.

- **While trying to add a range of numbers to a profile, PhoneSweep only adds a sub-range of the numbers**. This is probably due to a boundary condition. Add the numbers that were missed separately, and contact Sandstorm Enterprises to report the problem. Note that in a single command, PhoneSweep Basic won't add more than 800 numbers, and PhoneSweep Plus won't add more than 10,000 numbers.
- **The system crashed while PhoneSweep was running and the database became corrupted**. This is an extremely rare condition, as the SQL database is tolerant of most system crashes. However, recovery tools are available. Before using them, make a copy of the corrupted directory. Then run the program *dbfix.exe* that is in the top-level PhoneSweep directory. Select the corrupted database from the list and the recovery tools will be run on the database.
- **The PhoneSweep report lists the scan as incomplete, even though the program says it is 100% complete.** When scanning for both fax machines and modems, if calls to a modem in data mode all result in Busy and PhoneSweep has made the maximum number of redials allowed, PhoneSweep will not be able to initiate a fax call to the number and will not be able to complete the scan. You can increase the value of Busy Redial on the **Dialing** sub-tab to complete the scan.
- **On the Status tab, the Elapsed Time shown does not correspond to the Time Until Finished.** This is normal. The Elapsed Time increases after PhoneSweep starts sweeping whether or not PhoneSweep is actually making calls, while Time Until Finished doesn't change unless calls are being made.
- **Call estimates seem unusually high.** The Calls Remaining value is estimated as a worst-case scenario. Before starting a sweep, it assumes that PhoneSweep will find a modem or fax machine on every number called. If a Single Call Detect (SCD) call doesn't find Fax or Carrier, PhoneSweep takes care of two projected calls with that one call and the Calls Remaining are reduced by two. For example, if you are running PhoneSweep in SCD mode to sweep two numbers, the initial value of Calls Remaining is four. If both numbers respond as Voice or Timeout, Calls Remaining will drop to two after the first call and zero after the second call.
- ***checkmodems.exe* finds the Modems, but PhoneSweep does not (when I check under the Modems sub-tab, the COM Ports are wrong).** When running *checkmodems.exe*, note what COM ports the modems are actually on. Then, go to the **Modems** sub-tab, and click on the box under Port column for the modem in question. This brings up a pull-down menu where you can select the correct COM port for each modem. Once you save any changes, PhoneSweep will find the modems. Further documentation can be found in Section 4.5, **Setting up your Modems**. If PhoneSweep continues to give you problems after this, please call PhoneSweep support.

PhoneSweep Error Messages

Error messages on install

- "**A required DLL file WS2_32.DLL was not found":** This means that you do not have WinSock 2.0 installed on your computer. Run the WinSock 2.0 installer *w95ws2setup.exe* that is located in the top-level PhoneSweep directory. You will need to reboot your computer after installing WinSock 2.0.
- **"Move data error":** This error indicates a problem with the installation CD-ROM itself. The CD-ROM could be scratched or have a defect that was not spotted during testing. If you encounter this error, contact Sandstorm Enterprises and request a replacement CD-ROM. In rare

cases, it may turn out that the manner in which the data is burned onto the CD-ROM is not compatible with your CD-ROM drive. Installing PhoneSweep by copying files from another computer may help, or Sandstorm may be able to help devise a workaround.

- **"The file *filename* is locked and not writeable":** During an installation, this means that some part of PhoneSweep was running and could not be overwritten. If the PhoneSweep User Interface is running, shut it down before attempting the install. If the debugging file *debug.bat* is running, close the DOS window it is using. If neither of these are running, hit CTRL-ALT-DEL to bring up the Task Manager and kill any processes named PhoneSweep or MySQLd. Alternatively, you can reboot your computer and begin the install again.
- **"PhoneSweep requires Administrator privileges on Windows NT"**: This indicates that you are installing PhoneSweep on a Windows NT system, but you do not have administrative privileges. Because PhoneSweep must install a service to interface with the hardware license manager, it must be installed by Administrator on Windows NT.
- **"d:\setup.exe not a valid NT program**.": Make sure you've selected the CDROM drive, and that it contains the PhoneSweep CD.
- **"Disabled Modem X, Cannot Open 'COM Y'.** If Checkmodems can find the Modems, Go to the **Modems** sub-tab, and see if PhoneSweep has the correct COM port selected. (Checkmodems will give you the COM ports that your modems are on. To change the COM port that PhoneSweep must use for a given modem, click on the box under Port column for each modem. You will be able to bring up a pull-down menu where you can select the correct COM port for each modem. Once you save any changes, PhoneSweep will find the modems. Further documentation can be found under "Setting up your Modems" in Section 4.5. If PhoneSweep continues to give you problems after this, please call Sandstorm.

Error messages on program startup

- **"A required file WS2_32.DLL was not found":** You do not have WinSock 2.0 installed on your computer. Run the WinSock 2.0 installer *w95ws2setup.exe*, which is located in the top-level PhoneSweep directory. You will need to reboot your computer after installing WinSock 2.0.
- **Any other error message stating that a DLL file could not be found:** Copying DLL files from one computer to another does not work. Try installing Internet Explorer 5.0 or upgrading to a newer service pack, which may provide the missing files.
- **"Another program is listening to TCP/IP port 4321. Do you have another copy of PhoneSweep running?":** Hit CTRL-ALT-DEL to bring up the Task Manager and select End Task for any programs called PhoneSweep or MySQLd, and then restart PhoneSweep.
- **"Sweep reports it could not open modem":** Run *checkmodems.exe* to find what COM ports have working modems attached to them. Use the Device Manager to determine the COM port, I/O address and IRQ the modem is on, and adjust the settings in the **Modems** sub-tab.
- **"Database server did not wake up":** The database server from the last time PhoneSweep was run could still be running. Hit CTRL-ALT-DEL to bring up the Task Manager and select End Task for any program called MySQLd. Then restart PhoneSweep. If this does not solve the problem, the network adapter (TCP/IP protocol stack) may not be correctly installed. You can install a network adapter via Control Panel to Network to Add Adapter to Microsoft to Dial-up Adapter.
- **"Required file: C:\Program Files\Sandstorm\PhoneSweep\profiles\mysql*filename.*isd is missing!"** Any of three files in this folder may be corrupted or missing. Reinstall PhoneSweep.

- **SQL errors on startup:** There are two main reasons why you may get an SQL error on startup. The most common is a problem with TCP/IP setup on your machine. A detailed troubleshooting guide for this can be found at http://www.sandstorm.net/support/phonesweep/mysql. The other reason may be a corrupt profile. See the troubleshooting guide for corrupt profiles at http://www.sandstorm.net/support/phonesweep/fixprofile.

Error messages regarding the dongle

- **"The PhoneSweep hardware license management device is no longer connected to the computer. PhoneSweep will no longer dial. Please reconnect the hardware license management device to enable PhoneSweep to dial"**: This message is displayed if the hardware license manager is not securely connected to the computer's parallel or USB port.

Error messages when starting a sweep

- **"No modems selected. You must select at least one modem in the Modems sub-tab under the** options **Setup tab before you can start sweeping"**: You may have tried to start a sweep without selecting any modems. Use the Modems sub-tab to select the modem(s) with which you wish PhoneSweep to dial.
- **"Modem is not responding.**": This error message indicates that the modem did not respond to an AT command. It is possible that the modem has entered an unexpected state. Power cycle the modem.

Error messages on the Status tab

- **"Disabled: <error message>":** Follow the steps below to diagnose the problem:
  - The error message will tell you why PhoneSweep was not able to use this modem. Check the **Status** tab and the **History** tab to determine the exact error message.
  - There may be a problem with your computer's COM: ports. Run checkmodems.exe to test your COM: ports.
  - The modem may not be turned on or plugged in (NO DIALTONE is an error message). Make sure that the modem is turned on and plugged firmly into a valid phone line. Remember that analog modems will not work when plugged directly into a digital phone line. If you have multiple modems and one is working, switch the working modem's phone line with the problem modem's phone line. If the previously working modem then experiences problems, the problem is with the phone line.
  - Many modems have two RJ11 backs on the back, one to hook into your phone system, one for an optional handset. Be sure you are using the proper jack, usually labeled "LINE."
  - There may be physical problems with the modem itself. If applications other than PhoneSweep cannot use the modem, the modem may be broken or defective, or incorrectly cabled.
  - If some modems connected via a Quatech PCI card stop working when the modems are moved around, check the connectors to see if they are loose. The connectors do not have screws to secure them to the modems.
- **"Cannot open COM: <number>":** This message usually means either that the PC does not have that COM: port installed or that some other application is currently using that particular COM: port. Run *checkmodems.exe* to further diagnose the problem.

Error messages on the History tab

- **"Modem reported modem error"**: Note whether the RD and SD lights on the modem are locked on. This may be a bug that showed up in PhoneSweep 1.1. Contact Sandstorm Enterprises to report the bug. Sandstorm has a patch, which may fix this bug.
- **"Problem with localwrite"**: This means that PhoneSweep failed in its attempts to communicate with a modem after a call had already begun. Check the connectors on the cables to your modems to see that they are firmly seated.

User interface error messages

- **"Can't run help system. Is hh.exe in the path? You can install it from hhupd.exe on the PhoneSweep CD":** There is an error in the Windows HTML help system. Reinstall it by running *hhupd.exe* in the top-level PhoneSweep directory.
- **"SHLWAPI.dll could not be found**": Install Internet Explorer 4.01 or higher.

The debug.bat File and Advanced Debugging

This interface is intended for advanced users familiar with TCP/IP and SQL. If you do not have this expertise, don't worry about running the tests in this section. If you have read carefully through the previous sections of the troubleshooting guide and have not solved your problem, please feel free to contact Sandstorm Technical Support by emailing *support@sandstorm.net*.

Running the file *debug.bat* presents you with a list of tests that you can perform to help diagnose problems with PhoneSweep. You can run this file by selecting **Troubleshooting Utility** from the Start / Programs / PhoneSweep menu. *Debug.bat* is in the top-level PhoneSweep directory and can execute the following tests:

- Initiate a TCP/IP ping of localhost, to see if the local protocol stack is available. PhoneSweep uses TCP/IP to communicate among the engine, database and UI.
- Start up the embedded SQL database separately from the PhoneSweep engine and UI, to test its behavior or to determine the precise error message from a failure.
- Start the PhoneSweep engine separately from the graphical user interface.
- Start the PhoneSweep UI separately from the engine and database.
- Check the status of an already-running copy of the SQL database.
- Log into the SQL database as administrator. This permits SQL queries directly to the database. This is intended for advanced users familiar with SQL.
- List all preference variables that have been set in the "default" profile directly from the SQL database.
- Run the dongle diagnostics program.
- Run the database fix program (DBFIX). This can repair a corrupt profile.

I've Tried Everything and PhoneSweep Still Doesn't Work!

First, check all the cables to the modems, and the phone jack wires that connect the modems to the phone lines. Make sure your modems are powered on. Second, reboot your PC. Windows itself can become unstable and cause problems for applications trying to run under it. If you are running PhoneSweep under Windows 95, NT, or 2000, try running PhoneSweep under Windows 98 instead. Users have historically reported fewer problems running PhoneSweep under Windows 98 than under Win95 or NT. If you are still having problems, contact Sandstorm Technical Support.

Appendix D: Contacting Sandstorm

This appendix describes how to contact PhoneSweep technical support and sales. We're always glad to hear from you. **Your comments are valuable to us -** much of this manual is based on input from PhoneSweep users. By telling us what features you want to see in PhoneSweep and working with us to resolve problems, you can help us deliver a product that lives up to your expectations.

About Technical Support for PhoneSweep

PhoneSweep comes with 60 days of free Support/Update service. You can purchase 12-month extensions of your Support/Update service either with your initial purchase of PhoneSweep, or later. If Sandstorm releases a new version of PhoneSweep during the period of your Support/Update contract, you will automatically receive the new version free of further charge.

Submitting Bug Reports

A Support/Update service contract is not required to submit bug reports. If you believe you have found a bug, please let us know so that we can fix it and deliver a better product. Sandstorm provides a web form at http://www.sandstorm.net/support/reportaproblem.shtml for convenient submission of bug reports.

Before You Contact Sandstorm Technical Support

Before contacting Sandstorm Enterprises Tech Support, please follow these two steps:

Look through the PhoneSweep Troubleshooting Guide. The Troubleshooting Guide contains a clear summary of many common problems with PhoneSweep and their solutions.

Have the following information readily available:

- Version number of your copy of PhoneSweep (1.1, 2.1, 3.01, 4.0, etc.) See the Help/About button in the main PhoneSweep window.
- What platform you were running PhoneSweep on at the time of the problem, including Operating System version and Service Pack level.
- The brand and model of the modem you were using to dial
- The CPU speed of the computer that had problems running PhoneSweep
- The amount of RAM in the computer that had problems running PhoneSweep
- Any error messages that PhoneSweep displayed at the time the problem occurred (Please try to get exact wording, as this can indicate the source of the problem).
- Also the Make/Models of any Multi-port and/or Network cards.
- Did PhoneSweep work on the same machine prior to this? Did something change?

Save the file *phonesweep.log*. Although we may not ask for it right away (it can be a very large file) we may request that you send it to us later for debugging purposes.

Contacting Sandstorm Technical Support

On the web: Go to http://www.sandstorm.net/support/reportaproblem.shtml. The technical support web page contains an automated system for asking technical questions and submitting bug reports.

By email: Send email to support@sandstorm.net.

By phone: You can reach Sandstorm Enterprises at (617) 426-5056. We are generally available to answer technical support questions between the hours of 9:00 AM and 5:00 PM US Eastern Time (GMT minus 5:00).

Contacting Sandstorm Sales

For pre-sales assistance, information about future versions of PhoneSweep, or to order products from Sandstorm, you can reach us in three ways:

Email: sales@sandstorm.net

Telephone: Call us at (617) 426-5056 between 9AM and 5PM US Eastern Time.

Fax: Fax us at (617) 357-6042

Appendix E: Architecture and the Command Line

Under normal circumstances, PhoneSweep's internal structure should be transparent to the user. However, in the event of complications, knowledge of the architecture may be helpful.

The program is started when the user double-clicks on the PhoneSweep engine executable. The PhoneSweep engine then launches the embedded SQL server and the PhoneSweep user interface.

The PhoneSweep program consists of three parts:

- **The PhoneSweep engine** (*phonesweep.exe*), a Win32 executable written in C.
- **The PhoneSweep embedded SQL database** (*dbm\bin\mysql.exe*).
- **The PhoneSweep user interface** (g*ui\ps.exe*), a Win32 executable written in C++ using the QT user interface library.

All of these components communicate using local TCP/IP data streams. Our implementation requires that the Windows Sockets API version 2 DLL be accessible, and that we can connect to ourselves using the Unix-style IP loopback address, 127.0.0.1.

Running PhoneSweep from MS-DOS

PhoneSweep can be run from an MS-DOS prompt. There is usually no reason to do so, but sometimes it can be useful when one is troubleshooting PhoneSweep. To run PhoneSweep this way, go to an MS-DOS prompt window and change directories to the PhoneSweep directory; then type <*phonesweep*><ENTER>. If you have installed PhoneSweep in the default directory, this will be

```
C:\Program Files\Sandstorm\PhoneSweep>phonesweep
```

PhoneSweep has a number of command line arguments that may be useful. They are listed in the chart below. To run PhoneSweep with a command line argument, change directories to the PhoneSweep directory, then type <*phonesweep*> <*arg1*> <*arg2*> etc. <ENTER>, where *arg1, arg2* etc. are the command line arguments you wish to invoke. For example, to run PhoneSweep in engine debugging mode and without displaying the splash logo upon startup, type:

```
phonesweep –enginegui -nosplash
```

PhoneSweep Command Line Arguments

-help	Lists the available command line arguments in a pop-up window; does not start PhoneSweep
-initialize	Erases all profiles currently stored on your system. Use this option with caution. You can perform the same function by dragging all of the directories beginning with “PS_” inside the Profiles directory into the trash. Do not drag the Profiles directory itself into the trash, as this will cause PhoneSweep to stop functioning.
-version	Display the version of the PhoneSweep executable in a pop-up window.
-nogui	Do not launch the GUI.
-enginegui	Display the engine’s debugging GUI.

-nosplash	Do not display the PhoneSweep splash screen.
-playbuild	Play the PhoneSweep build number in touch-tones through the computer's speaker upon startup.
-noantispoof	Disable the requirement for an antispoof response on API connections
-foreign	Allow the engine to accept connections from IP addresses other than 127.0.0.1. Use with caution.
-logres	Log all commands sent to the PhoneSweep engine over the API, as well as all responses.
-simulate	Run the simulator, rather than the real dialer.
-sqltrace	Log all SQL queries and results to the *phonesweep.log* file.
-profile <*profilename*>	Start PhoneSweep with the specified existing profile loaded.
-newprofile <*profilename*>	Start PhoneSweep with a new, named profile.
-listprofiles	Display a list of existing profiles without actually starting PhoneSweep.

Environment Variables

As well as entering arguments on the command line, you can save your preferred combinations of arguments in an environment variable called PSOPTS in the *autoexec.bat* file. For example, if you want the PhoneSweep splash screen to never be displayed, enter the following line into your *autoexec.bat* file:

```
SET PSOPTS=-nosplash
```

Appendix F. Sample *brutecreate.exe* Output File.

For input, *brutecreate.exe* uses the following two files:

- *unametest.txt*, with contents:*

```
root

guest
usera
admin
userb
```

- *pwdstest.txt*, with contents:*

```
password
secret
toor
changeme

guest
```

*Note: to use a blank (NULL) user name or password, simply type a carriage return on a line. A single space will require that you type a space then carriage return.

First, clear the existing *bruteforce.txt* file by issuing the **clear** command (from an MS-DOS prompt):

```
brutecreate clear
```

Then combine the two files by issuing the **combine** usernamefile.txt passwordfile.txt command.

```
brutecreate combine unametest.txt pwdstest.txt
```

The usernames file is simply a text file list of usernames, with each user name on its own line ending in a carriage return. To use a NULL or empty username, simply use a carriage return for that line. (You do not need to bracket each user name with double quotes.)

The password file is simply a text file list of passwords, with each password on its own line ending with a carriage return. To use a NULL or empty password, simply use a carriage return for that line. (You do not need to bracket each password with double quotes.)

Brutecreate combine will add the double quotes around both usernames and passwords.

The *bruteforce.txt* file created is shown on the next page. Note that the total number of entries is the product of the number of usernames and the number of passwords, in this case 25. Keep in mind how many username/password combinations are created by *brutecreate*.exe, and that PhoneSweep in Penetrate mode will try all these combinations for each system it identifies.

bruteforce.txt, as generated by the Brutecreate.exe combine option:

```
"root" "password"
"root" "secret"
"root" "toor"
"root" "changeme"
“root” “”
"root" "guest"

“” “password”
“” “secret”
“” “toor”
“” “changeme”
“” “”
“” “guest”

"guest" "password"
"guest" "secret"
"guest" "toor"
"guest" "changeme"
“guest” “”
"guest" "guest"

"usera" "password"
"usera" "secret"
"usera" "toor"
"usera" "changeme"
“usera” “”
"usera" "guest"

"admin" "password"
"admin" "secret"
"admin" "toor"
"admin" "changeme"
“admin” “”
"admin" "guest"

"userb" "password"
"userb" "secret"
"userb" "toor"
"userb" "changeme"
“userb” “”
"userb" "guest"
```

By adding **flip** at the end of the **combine usernamefile.txt passwordfile.txt** command, Brutecreate will add a line for each username with the username backwards as a password. Thus you would type:

```
brutecreate combine username.txt passwords.txt flip
```

Appendix G: A Sample Standard PhoneSweep Report

Executive Summary of PhoneSweep Scan

Profile Name:	SAMPLE_REPORT
Report Generated:	Thursday, March 16 2000 12:17:52
Time of First Call:	Wednesday, March 15 2000 13:44:28
Time of Last Call:	Wednesday, March 15 2000 13:53:06
Elapsed Time During Scan:	9 minutes, 3 seconds
Phone Numbers Assigned to Dial:	5
Number of calls made:	12
Phone Numbers Dialed using Single Call Detect™:	5
Phone Numbers Dialed using Data-only Mode:	1
Phone Numbers Dialed using Fax-only Mode:	0
Phone Numbers Checked for Data:	5
Phone Numbers Checked for Fax:	5
Search for modems completed:	100.0%
Search for fax machines completed:	100.0%
Username/password guessing completed:	n/a
Modems found:	1
Systems compromised:	n/a

When the report was generated, PhoneSweep was configured to scan for both fax machines and modems. PhoneSweep was configured to only connect to and identify modems, but not to attempt to penetrate them.

Engineering Summary of PhoneSweep Scan

Profile Name:	SAMPLE_REPORT
Scan Started:	Wednesday, March 15 2000 13:44:28
Scan Stopped:	Wednesday, March 15 2000 13:53:06
Elapsed time:	9 minutes, 3 seconds
Report Generated:	Thursday, March 16 2000 12:17:52

Introduction:

PhoneSweep is a program developed by Sandstorm Enterprises (http://www.sandstorm.net) to search for modems within a set of phone numbers. PhoneSweep attempts to identify systems attached to remote modems as well as attempting to find areas of poor security by guessing common usernames and passwords.

Some modems are of higher quality than others, and can report more information about a remote phone number. These modems can recognize remote fax machines, phones answered by human beings, or simply just when a remote number is ringing. Sandstorm Enterprises, Inc. makes available a recommended modem list, including modems known to work well with PhoneSweep

Without a recommended modem, PhoneSweep must rely on a time-based timeout to end a connection. It will only be able to differentiate between calls to modems, busy signals, and calls that timed out. PhoneSweep will not then include a list of fax, voice, and ring timeout numbers.

PhoneSweep Terminology:

Term	Definition
Anomaly	An "anomaly" is a PhoneSweep result that is not consistent and should be investigated. For instance, if a phone number is answered once with "carrier" (answered by a modem) but later on answered by a human voice, this is an anomaly and may indicate an unauthorized modem.
Brute force password guessing	"Brute Force" username password guessing means that PhoneSweep will call a remote number, and offer one of its assigned username/password pairs.
Compromised or Penetrated	A system has been "compromised" or "penetrated" if PhoneSweep was able to guess a valid username and password for that system.
PhoneSweep	A program developed by Sandstorm Enterprises (www.sandstorm.net) to search for modems within a set of phone numbers. PhoneSweep can attempt to identify systems attached to remote modems as well as attempting to find areas of poor security by guessing common usernames and passwords.
Scan or Sweep	A PhoneSweep "scan" or "sweep" is a series of calls to a list of assigned numbers to search for modems, and possibly to attempt to penetrate those modems.
Username/password recycling	If PhoneSweep is "recycling" usernames and passwords, then it will attempt to brute force its entire list on **each** modem that it finds. If it is not recycling, it will use each username/password pair on its list only once.

Call Response States:

Call response state	Explanation
Busy	This phone number was always busy when dialed. If a busy number is later redialed and is not busy, it is listed under the other category.
Carrier	The remote phone number responded with a carrier signal; an electronic signal that indicates a computer is attached to the other end. A carrier signal means that electronic data transfer between two computers is possible, which may mean that network-based security can be evaded. Numbers with "carrier" are also referred to as numbers with modems attached.
Fax	A fax machine answered the remote phone line.
Ring Timeout	If your modem can detect when a remote phone number is ringing, PhoneSweep will record calls that ring past a limit as "Ring Timeout". The ring limit varies based on the time period during which the phone number was called.
Screened	A phone number is "screened" if the first part of the number is "9911" or "911". Screening is designed to prevent accidental calls to emergency numbers in certain countries, including the United States and Canada.
Timeout	PhoneSweep has timeout settings that vary depending on the time period in which the phone number was dialed. If the remote number is not ringing (or your modem cannot detect rings), and nothing answers the phone, the call times out.

Tone	The remote phone number answered with a dial tone. “Tone” calls may indicate a number that an outside person may use to make toll calls at your expense, and should be checked to make sure that they cannot be misused.
Voice	If you have a modem that can detect voice, then PhoneSweep will mark human-answered calls as “voice”. Answering machines and voicemail systems will also qualify as voice.

Dialed Phone Numbers:

	Total Phone Numbers With This Result	Percent of Total Phone Numbers
Assigned to Dial	5	100.0%*
Checked for Data	5	100.0%*
Carrier	1	20.0%
Tone	1	20.0%
Busy	1	20.0%
Ring Timeout	0	0.0%
Timeout	0	0.0%
Voice	2	40.0%
Screened	0	0.0%

* As a percent of the total numbers assigned to dial, as opposed to actually dialed.

The percentages may not add to 100 percent and there may be more distinct results than assigned phone numbers. This can happen if a phone number responded in two different ways. Also, if the scan was not completed, the numbers will be less than 100 percent.

Discovered Fax Machines:

	Total Phone Numbers With This Result	Percent of Total Phone Numbers
Assigned to Dial	5	100.0%
Checked for Fax	5	100.0%
Faxes found:	0	0.0%
Screened:	0	0.0%

Discovered Modems:

	Total Phone Numbers With This Result	Percent of Phone Numbers With Carrier
Numbers with Carrier:	1	100.0%
Identified	1	100.0%
Unidentified	0	0.0%

Penetrated Modems:

	Count of systems penetrated	Percent of total penetrated systems
Penetrated Systems	n/a	n/a
Identified	n/a	n/a
Unidentified	n/a	n/a

Percent of Brute force username/password guessing attempts completed: n/a

Anomalies:

1-555-555-6650 was identified as the following different systems: Annex Remote Access Server, Cisco

Systems Penetrated by PhoneSweep:

PhoneSweep did not succeed in penetrating any systems.

Carrier Numbers Found:

The following numbers responded with a modem carrier, allowing access to that system. This means that an outside person may be able to connect to your network through these numbers.

We recommend that you compare with known modem numbers, and that all modem lines be further checked to be sure that strong security is in place. Examples of poor modem security include (but are not limited to) systems without any passwords or systems with well-known or easily guessed usernames and passwords.

1-555-555-6650

Busy Numbers Found:

The following numbers were always busy when called by PhoneSweep. They may be leased lines, or be voice or data lines that happened to be busy whenever PhoneSweep checked them. We recommend these numbers be checked further to ensure that they are not unauthorized modems.

1-555-555-6651

These always busy telephone numbers can be re-scanned by increasing the **Busy Redial** value on the **Dialing** sub-tab. When this report was generated, **Busy Redial** was set to 5.

Tone Numbers Found:

The following numbers returned a second dial tone when called by PhoneSweep. These numbers should be closely checked to ensure that outsiders cannot make calls through an internal exchange. If these tone numbers allow long-distance or international calls, you may be a target for expensive telephone fraud.

9--

Fax Numbers Found:

The following numbers responded with a FAX tone when PhoneSweep scanned them. FAX machines do not represent a security risk, although FAX numbers which also responded with Carrier could be unauthorized or misconfigured fax/modems.

No fax machines were found during this PhoneSweep scan.

Incomplete Scan Areas:

The PhoneSweep scan was complete.

Identified Systems with Modems:

1-555-555-6650 - Annex Remote Access Server

1-555-555-6650 - Cisco

Unidentified Carrier Numbers:

PhoneSweep did not discover any modems it could not identify during this sweep.

Responses from Penetrated Systems:

No responses were received from penetrated modems during this PhoneSweep scan.

Appendix A: Responses from target modems

1-555-555-6650 1999-06-30 13:47:34

ATDT 1-555-555-6650

CONNECT 9600

Welcome to sample.isp, router #1

Type "PPP DEFAULT" to go into PPP mode.

Type "telnet {host}" to telnet to a host.

For further information, please talk to your ISP reseller, or call us

at 555-555-6688.

-Sample.isp.

User Access Verification

Username:

1-555-555-6650 1999-06-30 13:51:00

ATDT 1-555-555-6650

CONNECT 9600

Annex Command Line Interpreter * Copyright (C) 1988, 1997 Bay Networks

Checking authorization, Please wait...

Appendix B: Phone Number Taxonomy

Number:	Result:
1-555-555-6650	CARRIER - Annex Remote Access Server
1-555-555-6650	CARRIER - Cisco
1-555-555-6651	BUSY
1-555-555-8989	VOICE
555-4120	VOICE
9--	TONE

Appendix C: List of all calls and their results

Call time:	Number:	Result:
Wednesday, June 30 1999 13:44:28	**9--**	TONE
Wednesday, June 30 1999 13:45:01	**1-555-555-6650**	NO_FACSIMILE
Wednesday, June 30 1999 13:46:41	**555-4120**	VOICE
Wednesday, June 30 1999 13:47:34	**1-555-555-6650**	CARRIER - Cisco
Wednesday, June 30 1999 13:48:15	**1-555-555-8989**	VOICE
Wednesday, June 30 1999 13:48:53	**1-555-555-6650**	NO_FACSIMILE
Wednesday, June 30 1999 13:50:33	**1-555-555-6651**	BUSY
Wednesday, June 30 1999 13:51:00	**1-555-555-6650**	CARRIER - Annex Remote Access Server
Wednesday, June 30 1999 13:51:45	**1-555-555-6651**	BUSY
Wednesday, June 30 1999 13:52:12	**1-555-555-6651**	BUSY
Wednesday, June 30 1999 13:52:39	**1-555-555-6651**	BUSY
Wednesday, June 30 1999 13:53:06	**1-555-555-6651**	BUSY

Appendix H: A Sample Differential PhoneSweep Report

Differential Executive Summary:

Report generated: Friday, May 12 2000 11:37:15

Old profile: **'PBX_MAY10'**

Started sweeping: Wednesday, May 10 2000 13:18:34

Stopped sweeping: Wednesday, May 10 2000 13:39:16

New profile: **'PBX_MAY12'**.

Started sweeping: Friday, May 12 2000 10:55:49

Stopped sweeping Friday, May 12 2000 11:34:11

The effort level for both scans was set to **Penetrate**.

Warning: **PBX_MAY10** was not configured to scan for fax machines, **PBX_MAY12** was.

Busy redial was set to **5** in both profiles.

Engineering Summary:

Introduction

PhoneSweep is a program developed by Sandstorm Enterprises (http://www.sandstorm.net) to search for modems within a set of phone numbers. If configured to do so, PhoneSweep attempts to identify systems attached to remote modems and can attempt to find areas of poor security by guessing user-defined common usernames and passwords.

This report is a 'differential' report; it displays the differences between two sweeps. One sweep has been designated as the 'older' sweep, the other as the 'newer' sweep. The differential report will highlight changes between the older sweep and the newer sweep.

Differential reports must be run over profiles with overlapping phone numbers; if the two profiles have no phone numbers in common, then no meaningful comparisons can be performed. If some numbers have been added or removed, then those differences will be reported.

Phone Number Differences:

Count of phone numbers that are in both profiles:

240

Both profiles used the same set of phone numbers.

Penetration Differences:

New successful penetrations with new usernames and passwords:

(Username/password pairs not tried in PBX_MAY10)

201: guest,guest - Good username Good password

Now failed penetrations that were successful in old profile 'PBX_MAY10'

415: root,toor - was Good username Good password, now Bad username or password

Call History Difference Summary:

New modems found in PBX_MAY12:

201: PC Anywhere, formerly Ring Timeout

Identification Differences:

Changes in identification:

Phone number	Results in 'PBX_MAY10'	Results in 'PBX_MAY12'
415	PPP (CHAP) IP: 128.127.126.125 (Peer: 10.0.0.2)	Unknown with login: prompt

Full Call History Change Report:

Changes from PBX_MAY10 to PBX_MAY12:

Phone Number	Old Call Result	New Call Result
201	Ring Timeout	Carrier

Appendix I: Miscellaneous

Password Security

You can have the best security in the world; however, if you have user who uses an easily guessed password, or machines that have the same user/Password combination, then the most advanced security will not protect your company's resources.

Passwords need to be simple enough to remember, yet not easily guessed by knowing something about the person who created the password For instance, the password that former President Clinton used for his e-signature when signing the e-signature bill was "Spot," the name of his cat. Anyone obtaining his card at that point could have easily broken in and used his Electronic Signature by simply throwing the names of his family and pets at the card.

Passwords should be about 7-10 characters long, consisting of a mix of letters and other characters. Taking some letters based on a phrase only the user knows and does not share, and then breaking the phrase up with non-alphabet characters in the middle can help both the user and you. Never base passwords on single entities, such as a show or favorite author; use combinations of two or more entities instead. And never use anything remotely related to one's own or familial names, birthdays or ages. Make sure that users with multiple accounts or access points have a unique password for each point (similar to not using the same 4-letter code for one's voice mail AND ATM accounts).

Manufacturer-supplied default passwords are another vulnerability. Always check that the manufacturer-supplied default passwords have been changed on each and every machine, and never allow anyone to use the same Username/Password combination on multiple machines in your company. It is one thing to use secure connection programs that allow users to get onto multiple boxes (such as TACACS for Cisco routers). It is another to have all the boxes default to the same passwords through other connection means. (Three Internet companies alone in 1990-2000 had security breaches because all machines had the same password for users. In once case, the manufacturer's default had never been changed.)

We have provided a basic list of common passwords and usernames in the *bruteforce.txt* file. In addition, there is a longer list of passwords in *largebrute.txt*, the same passwords spelled backwards in *largebruteback.txt*, and default system passwords for a variety of systems in *systemdefault.txt*.

Online resources regarding password security:

- Vislab's Common Password Guidelines: http://www.vislab.ua.edu/Common/Passwords.html
- "Techniques Adopted By 'System Crackers' When Attempting To Break Into Corporate or Sensitive Private Networks." From Network Security Solutions Ltd. Front-line Information Security Team (FIST), December 1998. http://www.ns2.co.uk/archive/FIST/papers/NSS-cracker.txt
- Papers on password security: http://www.packetstormsecurity.org/papers/password/
- DoD password guidelines: http://www.packetstormsecurity.org/papers/password/dodpwman.txt
- Password cracking FAQ: http://www.password-crackers.com/pwdcrackfaq.html
- Password cracking Tools: http://www.password-crackers.com/pwdcracking.html

- Hackers Club Home Page: http://hackersclub.com/km/files
  - http://hackersclub.com/km/files/password_cracker/wordlists
  - http://hackersclub.com/km/files/password_cracker/wordlists/common-passwords.txt
- UC DAVIS's password security guidelines: http://it.ucdavis.edu/pubs/quicktips/password.html
- Phrack Magazine: http://www.phrack.org (Going through all back issues is recommended.)

List of Identified Systems

As of July 18, 2002, PhoneSweep can identify 468 systems:

3Com Multiprotocol Communications Server
3Com SuperStack II Remote Access System
3Com SuperStack II Remote Access System 1500
3Com SuperStack System
3Com Total Control HiPer ARC Platform
3Com Total Control Platform
ACCULINK 3165/3166 T1/FT1 DSU/CSU
ACCULINK Access Controller
ADC Kentrox
ADC Kentrox AAC Manager ATM Access Device
ADC Kentrox AAC-1 ATM Access Device
ADC Kentrox AAC-1 Version 2.71 ATM Access Device
ADC Kentrox AAC-2 ATM Access Device
ADC Kentrox AAC-3 ATM Access Device
ADC Kentrox CellSMART ATM Access Device
ADC Kentrox CellSMART Version 2.71 ATM Access Device
ADC Kentrox CellSMART Version 3.00 ATM Access Device
ADC Kentrox CrossPATH CSU
ADC Kentrox CrossPATH II CSU
ADC Kentrox DataSMART System
ADC Kentrox DataSMART T3 SMDSU
ADC Kentrox DataSmart
ADC Kentrox Device
AHC System
AMS Pick64
AMS Pick64+ 2.3
AT&T 386 UNIX
AT&T Dataphone II Network Service Controller
AUDIX Voice Messaging System
AccessBuilder 4000
AccessBuilder System
Advanced PICK
Advanced PICK O/S
Advanced PICK O/S v.6.1
Advanced PICK O/S v.6.x
Alcyon System
Alphanumeric paging system
Annex Remote Access Server
Anodyne BBS
Apertus System
Aquatrac Instruments Water Treatment Controller
Ascend (Lucent) MAX Concentrator
Ascend MAX 3000 Concentrator
Ascend MAX 4000 Concentrator
Ascend MAX 4046 Terminal Server
Ascend MAX 4048 RAC Terminal Server
Ascend MAX 4048 Terminal Server
Ascend MAX Terminal Server
Ascend MAX200 Terminal Server
Ascend Pipeline Terminal Server
Ascend Terminal Server
Autonet dialup port
BITCOM Host
BITCOM for DOS, Bit Software, Inc.
BITCOM for Windows, BIT Software, Inc.
BITCOM for Windows, Bit Software, Inc.
BLAST
BSD/OS (UNIX)
Bay Technical Associates Data Switch
Bay Technical Associates Data Switch Series F.0.36
BayNetworks Accelar 1200 Routing Switch
BayNetworks Accelar 1250 Routing Switch
BayNetworks Accelar Series Routing Switch
BayNetworks BayStack 350 Switch
BayNetworks BayStack 450 Switch
BayNetworks BayStack 450 Switch (12 port)
BayNetworks BayStack 450 Switch (24 port)
BayNetworks BayStack Series Switch
BayNetworks System
BinkleyTerm Mail Interface and Dumb Terminal Package
BinkleyTerm Version 2.30 Mail Interface and Dumb Terminal Package

BinkleyTerm Version 2.50 Mail Interface and Dumb Terminal Package
BinkleyTerm Version 2.60 Mail Interface and Dumb Terminal Package
BinkleyTerm XE Version 2.60 Mail Interface and Dumb Terminal Package
Brite Voice System
Building Automation System w/o password
COMSPHERE 6700 Series Network Management System
CRC Netpath 100 Frame Relay
CRC Netpath 64 Frame Relay
Carbon Copy
Chase Research IOLAN Terminal Server
Cisco
Cisco 3640 Router
Cisco Catalyst or Router
Cisco Terminal Server (no authentication required)
Cisco system, left logged in
Citrix ICA WinFrame
Cognitronics Announcer
Cognitronics System
Computer Process Controls System
Computerm VMC (Virtual Mainframe Channel) 8100 channel extension system
Computerm VMC (Virtual Mainframe Channel) 8250 channel extension system
Computone Intelliserver Terminal Server
Computone Terminal Server
Concentric.net Dialup
Control Data Corporation Network Operating System
Convergent Technologies CTIX (UNIX)
CrossComm Corp ILAN XL Switch or Router
Cubix System
Cubix WorldDesk
DCP Extender
DECserver 200 Terminal Server
DECserver System
DG/UX (UNIX)
DG/UX Release 1.5 (UNIX)
DG/UX Release 2.0 (UNIX)
DG/UX Release 2.x (UNIX)
DG/UX Release 3.0 (UNIX)
DG/UX Release 4 (UNIX)
DG/UX Release 4.11(UNIX)
DG/UX Release 4.2 (UNIX)
DG/UX Release 4.3 (UNIX)
DG/UX Release 4.x (UNIX)
DIALOG network dialup
DIGI International LANA Server
DIGI International LANA Server 10e
DIGI International LANA Server 23
DIGI International LANA Server 8e
DRS/NX 6000 (UNIX)
DRS/NX System (UNIX)
DUNSNET dialup port (Dun & Bradstreet)
DYNIX System (UNIX)
DYNIX System V.2.1.2 (UNIX)
DYNIX System V.2.1.x (UNIX)
DYNIX System V.2.x (UNIX)
Data General AOS/VS System
Data General System
Data General System MV/5500
Data General's DG/UX (UNIX)
Datafaction, Inc. Accounting System login
Datafaction, Inc. System Software
Datataker Data Logger
Defender 5000 Callback System
Defender Challenge Response System
Defender Security Server
Definite Solutions FrontDoor BBS
Definite Solutions FrontDoor Version 2.12
Definite Solutions FrontDoor Version 2.12 Shareware
Definite Solutions FrontDoor Version 2.26
Definite Solutions FrontDoor Version 2.26 Shareware
Dell UNIX System V
Digital OpenVMS Alpha
Digital OpenVMS System
Digital OpenVMS VAX
Digital Research Concurrent DOS system
Digital Speech Systems TMX Series voice mail system
Digital Speech Systems TMX-12/500 voice mail system
Digital Speech Systems UniVoice 100 voice mail system
Digital Ultrix (UNIX)
Digital VAX System
Digital VAX/VMS
Digital VMS System
Digital VaxCluster (VMS)
Electrotek Concepts Power Quality Network
Emulex ConnectPlus LT Remote Access Server
Emulex ConnectPlus System
Erehwon Zipster Modem (GeCOS)
Excalibur BBS
Executone Information Systems, System IDS
Executone PBX

Federal Government Computer System
FirstClass BBS
Fluidmaster Inc. Control
Fluidmaster Inc. Control on ST1000 System
FreOS, version 1.2
FreeBSD (UNIX)
FrontDoor Mail Suite
FrontDoor version 1.99 Mail Suite
FrontDoor version 2.02 Mail Suite
FrontDoor version 2.12 Mail Suite
FrontDoor version 2.25 Mail Suite
FrontDoor version 2.30 Mail Suite
GCM System
Gandalf Starmaster network
General Automation Power95 control system (PICK Environment)
General Automation R91 control system (PICK Environment)
General Automation ZEBRA
General Automation control system (PICK Environment)
General Electric Company Controlle
General Electric Company System
Generic IBM system, possibly IBM OS
Generic IBM system, possibly mainframe
Global Water Field Data Logger System
HADAX Electronics, Inc Intelliswitch System Series 2000
HADAX Electronics, Inc. Device
HP Remote Assistant
HP System
HP-UX (UNIX)
HP9000 Console Prompt
Hermes II Macintosh BBS
Hewlett Packard System (Possibly Unix)
Hewlett-Packard MPE/XL System
Hewlett-Packard MPE/iX System
Hilgraeve HyperACCESS Communications Software
Hilgraeve HyperACCESS Communications Software for OS/2
Hilgraeve HyperACCESS Lite Communications Software for OS/2
Hilgraeve HyperACCESS PRO Communications Software
Hilgraeve HyperACCESS Pro Communications Software for OS/2
Hilgraeve HyperACCESS for Windows 95 and NT
Hilgraeve HyperACCESS/5 Communications Software
Hilgraeve HyperHost Communications Software
Hilgraeve HyperHost Communications Software for OS/2
Homecare Management System
IBM 3174 Control Unit Emulator
IBM 3174 Control Unit Emulator, ver. 7.03
IBM 3174 Control Unit Emulator, ver. 7.x
IBM 3708
IBM 5251 Terminal
IBM 8235 with NL
IBM 8235 with RET
IBM AIX (UNIX)
IBM AIX (Unix) with PICK's D3 Database System
IBM AIX Version 2 (UNIX)
IBM AIX Version 2.2 (UNIX)
IBM AIX Version 2.x (UNIX)
IBM AIX Version 3 (UNIX)
IBM AIX Version 3 (UNIX)on RISK System 6000
IBM AIX Version 4 (UNIX)
IBM PhoneMail
IBM RS/6000 with Pick's D3 Database Management System
IBM System/32
IBM System/88
Infonet DialXpress
Inter-Tel IMX 1224/2460 Key Telephone System
Inter-Tel IMX Key Telephone System
InterLynx/5251
InterSystems MSM-PC/PLUS
Intersystems Inc.'s DT-MAX 4.3M for the Data Tree MUMPS database and runtime system
Intersystems Inc.'s DT-MAX 4.8 for the Data Tree MUMPS database and runtime system
Intersystems Inc.'s DT-MAX for the Data Tree MUMPS database and runtime system
Intersystems Inc.'s DTM-MAX for the Data Tree MUMPS database and runtime system
Intersystems Inc.'s DTM-PC for the Data Tree MUMPS database and runtime system
Lansource WINport
Lantronix
Lantronix EPS-1 Print Server
Lantronix EPS-2 Print Server
Lantronix EPS-4 Print Server
Lantronix LPS Micro Print Server
Lantronix Multi-Protocol Micro Print Server
Libra Systems Corp. Quarry Master 2 Plus
Lighthouse Power Switch
Lighthouse System

Linux System (UNIX)
Lithonia Synergy Lighting System Controller
Lucent PortMaster PM3
MANAKON Telemanagement Console
MAXIMUS BBS, version 2
MAXIMUS BBS, version 3
MAXIMUS BBS, version 3.01
MEGAHOST BBS
MIT Project Athena
MUMPS-systems 3.0.6 for a IBM/PC platform
MUMPS-systems for a IBM/PC platform
Management Information Base
Mecury Mail to AT&T Mail Gateway
MediaGate EdgeCommander
MediaGate System
MediaHost by MediaHouse Software Inc.
Mentor PRO integrated database environment
Mercury Coporation Mecury Mini-Max Electronic Volume Corrector
Mercury Corporation MERCOR EC Electronic Volume Corrector
Mercury Corporation MERCOR EC or EC-AT Electronic Volume Corrector
Mercury Corporation MERCOR EC-AT Electronic Volume Corrector
Mercury Corporation MERCOR MARK III Electronic Volume Corrector
Mercury Corporation MERCOR Mini-PT Electronic Volume Corrector
MichTron BBS
Microsoft Mail to AT&T Mail Gateway
Microware OS-9
NCR 386/486 UNIX
NLynx AXCESS/400 - V2.60
NLynx AXCESS/400 System
NLynx DATALYNX System
NLynx DATALYNX/400 - V3.00
NLynx DATALYNX/400 System
NLynx INTERLYNX 400 PLUS
NLynx INTERLYNX/400
NLynx INTERLYNX/400 - V2.17U2
NLynx INTERLYNX/400 - V2.22U2
NLynx INTERLYNX/400 - V2.22U3
NLynx INTERLYNX/400 - V2.60
NLynx InterLynx System
NLynx InterLynx/400
NeXTSTEP / NXFax System (UNIX)
NeXTSTEP System (UNIX)
Net Op no Prompt for password
Net Op with Prompt for Password
NetOP remote control system
NetWare CONNECT Service Selector
Netlink OmniLinx Switch
Network Access SW (Digital VAX cluster terminal server)
Newbridge 3600 MainStreet
Newbridge 3624 MainStreet
Newbridge MainStreet system
Newbridge Networks, possibly MainStreet
Northern Telecom SL-1
Novell Internet Access Server (NAIS)
Novell Internet Access Server (NAIS) v.4.1.0
Novell Internet Access Server (NAIS) v.4.1.x
Novell Internet Access Server (NAIS) v.4.x
OS/2 (UNIX)
OSICOM FPX4802/DES Frame Relay Encryptor
Octel System
Octel Voice Processing System
Open M System
Open M for MS-DOS
PC Anywhere
PC Anywhere (No password!)
PCBoard BBS
PICK O/S System
PPP
PPP (MajorTCP/IP by Vircom Inc
PROMIS II System
Paradyne 3510 Series DSU
Paradyne 3550/3551 DSU
Paradyne 3610 Series DSU
Paradyne 3615 Series DSU
Paradyne's ACCULINK 3100 Series Product Matrix
Paradyne's ACCULINK 3150 ESF T1 CSU
Paradyne's ACCULINK 3160/3164 DSU/CSU
Paradyne's ACCULINK 3162 T1/FT1 DSU/CSU
Paradyne's ACCULINK 317X Series E1 CSU/DSU
Paradyne's COMSPHERE 3600 Series DSU
Paradyne's NextEDGE Multiservices Access System
Pentium SCO Unix (UNIX)
Perle 394 Remove Controller
Perle Model 3i PC Dial-up Server
PhoneMail System
Picker IQ System
Port Master Prompt
Portmaster1 Terminal Server
Possible Alarm System
Possible Bulletin Board System (BBS)
Possible Cisco 2500 without password
Possible Cisco router without password

Possible Key Telephone Switch
Possible PICK Environment
Possible Scicom system
Possible Telephone PBX
Possible X.25 PAD
Possibly ProComm,spelled ProCom
Premier ESP Key Telephone System
Premisys IMACS Digital Telephone Switch
Premisys IMACS/600 Digital Telephone Switch
Premisys IMACS/800 Digital Telephone Switch
Premisys IMACS/900 Digital Telephone Switch
ProBoard BBS
Procomm
Procomm Plus
Procomm Plus for Windows
Procomm System
QNX Realtime OS
QuickMail
R91 Enhanced PICK
RAD Communications DXC-10A MultiService Access Node
RAD Communications DXC-30 MultiService Access Node
RAD Communications DXC-8R MultiService Access Node
RBSS Version 17.4 (Remote Bulletin Board System)
RBSS Version 17.4 with CDOOR MODS (Remote Bulletin Board System)
RBSS Version 17.5
ROLM PhoneMail
ROLM System
Red Hat Linux (UNIX)
Regulus System
Remote2 Host
Renex System
Renex TMS-3
Renex TMS-4
SAGE System
SCO Open Desktop (UNIX)
SCO Open Server Enterprise (UNIX)
SCO OpenServer (UNIX)
SCO System (UNIX)
SCO UNIX System V/386
SCO Unix (UNIX)
SCO UnixWare Version 2.1.1
SCO UnixWare Version 2.x
SCO UnixWare Version 7
SGI IRIX (UNIX)
SOTAS Circuitsentry
Santronics Software Wildcat! Interactive Net Server
Schindler Elevator Corp. Lobby Monitor
Searchlight BBS
Searchlight BBS (TeleGrafix Communications, Inc.)
SecurID Prompt
SecurID Protected
Secure Sentinel
Sentinel 2000
Sentinel 2000 access control system
Shiva LanRover
Siemens ROLM CBX
Siemens ROLM Remote Shelf
Siemens ROLM Remote Shelf (RMS2/RCM)
Siemens ROLM System
Siemens/ROLM CBX 8004 PBX
Siemens/ROLM CBX 9004 PBX
Siemens/ROLM CBX 9005 PBX
Siemens/ROLM System
Stac ReachOut
Sun Solaris (UNIX)
SunOS (UNIX)
Sunsoft INTERACTIVE UNIX
SuperDOS
System 5.4 (UNIX)
System V.4 (UNIX)
TELENET dialup port
TRIAD System
TRT Multispeed Device
Tandem Advanced Command Language Server
Telco Systems Inc. Route-24
Telco Systems Inc. System
TeleFinder BBS
Telebit ACS
Telebit NetBlazer
Telebit NetBlazer (possibly unconfigured)
Telebit NetBlazer version 3.0
Telrad Digital Key BX PBX
Tenon MachTen (UNIX for Mac)
TimePlex SYNCHRONY Enterprise Router
TimePlex System
Tracer 100 Building Control System
TriBBS
Triad Systems System
TxPORT Automatic Protection Switch
TxPORT Device
UNIX System
UNIX or Cisco System
US Robotics Courier Dial Security Session
US Robotics Courier Fax Dial Security Session

US Robotics Courier Modem
US Robotics V.Everything Dial Security Session
US Robotics V.Everything Fax Dial Security Session
US Robotics V.Everything Security Session
USL Unix System V
UUPC (UUCP client software)
UUPC (UUCP client software) for MS-DOS v. 5.00
Ultimate PLUS
Unidentified Acculink device
Unidentified Paradyne COMSPHERE device
Unidentified Paradyne device
Unidentified System with Login: prompt
UnixWare
VAIS FirstLine Voice Scripts
VERITAS Software Remote Access
VISTA Terminal Server VCP-1000 v1.272
Virtual Advanced BBS
WESCOM II Branch System
WESCOM Phone System
WILDCAT! BBS
Wang VS
WebFlow System
WellFleet (Bay Networks) System, left logged in
Wellfleet System
Western Telematic INCS-64 Data Switch
Western Telematic PollCat III PBX data recorder
Western Telematic PollCat NetLink PBX data recorder
Western Telematic PollCat PBX data recorder
Wildcat! BBS for Win95/NT
Worldgroup BBS
XETA System
Xenix system (Unix)
Xylogic Annex Remote Access Server
Xylogics Annex Remote Access Server
Xylogics System
Xyplex System
Xyplex Terminal Server
Xyplex Terminal Server (prompt)
Yale ASCII Terminal connected to IBM Mainframe
Yale ASCII Terminal connected to IBM Mainframe, ver. 2.1

Important Web sites and Phone Numbers

Sandstorm Enterprises *(617-426-5056) :* http://www.sandstorm.net

Recommended Modems: http://www.sandstorm.net/support/phonesweep/recmodems.shtml

Recommended Serial I/O cards: http://www.sandstorm.net/support/phonesweep/multiport.shtml

PhoneSweep FAQ: http://www.sandstorm.net/support/phonesweep/faq.shtml

Modems and Your Security Policy: http://www.sandstorm.net/products/phonesweep/modempolicy/

Multiport Card Vendors

SeaLevel *(SeaLevel VersaCom +4 (7401) and +8 (7801)Serial I/O multiport cards):* http://www.sealevel.com

Installation Note: You must first install asynchronous drivers before installing serial I/O card and attach the octopus cable. IMPORTANT: If you are putting your multiport card on a Windows 2000 system, go to the SeaLevel website to get the **latest** drivers. Earlier drivers can cause the system to freeze.

4 port cards: http://www.sealevel.com/catalog/4portpcia.htm

8 port cards: http://www.sealevel.com/catalog/8portpcia.htm

Drivers: http://www.sealevel.com/catalog/asyncsw.htm

Quatech *(Quatech QSP 100 4 port PCMCIA serial I/O adaptor with cable for laptops)* http://www.quatech.com

Modem Vendors

Zoltrix/Zoltix *(Zoltrix Rainbow 56K modem, FM-VSP56e2 and FM-VSP56e3)* http://www.zoltrix.com or http://www.zoltrix-int.com (International Web Site)

Installation notes: PhoneSweep does not use the drivers that come with your modem. However, to prevent the Add New Hardware wizard from coming up every time you restart your PC or laptop, we recommend that you install the modem drivers, then turn them off under Modem Properties in the System Devices panel found under Start->Settings->Control Panel. Sandstorm does sell Rainbow Modems if you are unable to find a nearby modem supplier in the U.S. or Canada.

Multi-Tech: *(Multi-Tech Systems MultiModem 56K Voice/Data/Fax (Multi-Tech MT5600ZDXV)* http://www.multitech.com and http://www.multitech.com/PRODUCTS/MultiModemZDX/

For ISDN: US Robotics External Courier Imodem: http://www.usr.com. Note: Site uses Java.

ScreenSaver Vendor

ScreenLock*: (Password protection/screen saver that allows programs to run in the background. Tested and approved for use with PhoneSweep)****:*** http://www.screenlock.com.